Instituto Serzedello Corrêa

Internet das coisas:

A proteção da privacidade em um mundo conectado

Manuella de Farias Nardelli Costa

Orientador: Prof. Dr. Bernardo Müller

Coletânea de Pós-Graduação, v.4 n.14

Governança e Controle da Regulação em infraestrutura

TRIBUNAL DE CONTAS DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL

TRIBUNAL DE CONTAS DA UNIÃO

MINISTROS

José Mucio Monteiro (Presidente)
Ana Arraes (Vice-presidente)
Walton Alencar Rodrigues
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz de Oliveira
Raimundo Carreiro
Bruno Dantas
Vital do Rêgo

MINISTROS-SUBSTITUTOS

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

Cristina Machado da Costa e Silva (Procuradora-Geral)
Lucas Rocha Furtado (Subprocurador-geral)
Paulo Soares Bugarin (Subprocurador-geral)
Marinus Eduardo de Vries Marsico (Procurador)
Júlio Marcelo de Oliveira (Procurador)
Sérgio Ricardo Costa Caribé (Procurador)
Rodrigo Medeiros de Lima (Procurador)

Instituto Serzedello Corrêa
Escola Superior do Tribunal de Contas da União

PROJETO GRÁFICO E CAPA
Núcleo de Comunicação - NCOM/ISC

Instituto Serzedello Corrêa
Escola Superior do Tribunal de Contas da União

PÓS-GRADUAÇÃO EM AUDITORIA FINANCEIRA

Internet das coisas:

A proteção da privacidade em um mundo conectado

Manuella de Farias Nardelli Costa

Orientador(a):
Prof. Dr. Bernardo Müller

Brasília | 2019

Resumo

O objetivo desse artigo é examinar a atuação do controle externo em relação a ferramentas consensuais de regulação, com foco na atuação do Tribunal de Contas da União (TCU) no caso de Termos de Ajustamento de Conduta (TAC) celebrados por Agências Reguladoras federais e nos limites dessa atuação. De modo a analisar a questão, foi realizada uma revisão da doutrina recente, legislação aplicável e jurisprudência do TCU. Com base em exame da legislação, verifica-se que o TCU tem competência constitucional e legal para analisar as atividades finalísticas das Agências Reguladoras, incluindo a celebração desse tipo de instrumento. A partir da revisão dos casos concretos, constatou-se que o TCU tem entendimento nesse sentido e já realizou o exame de alguns TACs celebrados por essas entidades, a exemplo da Anatel e da ANTT. Com base em análise crítica dessas deliberações, observa-se que o referido Tribunal tem seguido a mesma premissa adotada para examinar as atividades finalísticas das Agências Reguladoras, que é de um controle de segunda ordem, sem substituir as competências dessas entidades. Com poucas exceções, constatou-se que não houve questionamentos relativos às decisões discricionárias das agências, mas foram analisados aspectos abarcados em suas competências, como a motivação e a fundamentação utilizada na celebração desses acordos, a clareza dos termos, bem como a utilização da metodologia com base em critérios técnicos e legais vigentes.

Palavras-chave: Controle externo; regulação consensual; termos de ajustamento de conduta.

Abstract

falta abstract

Sumário

1. Introdução

O advento da Internet das Coisas tem ampliado a preocupação dos indivíduos acerca da sua vulnerabilidade diante da introdução de novas tecnologias em diversos campos do seu cotidiano.

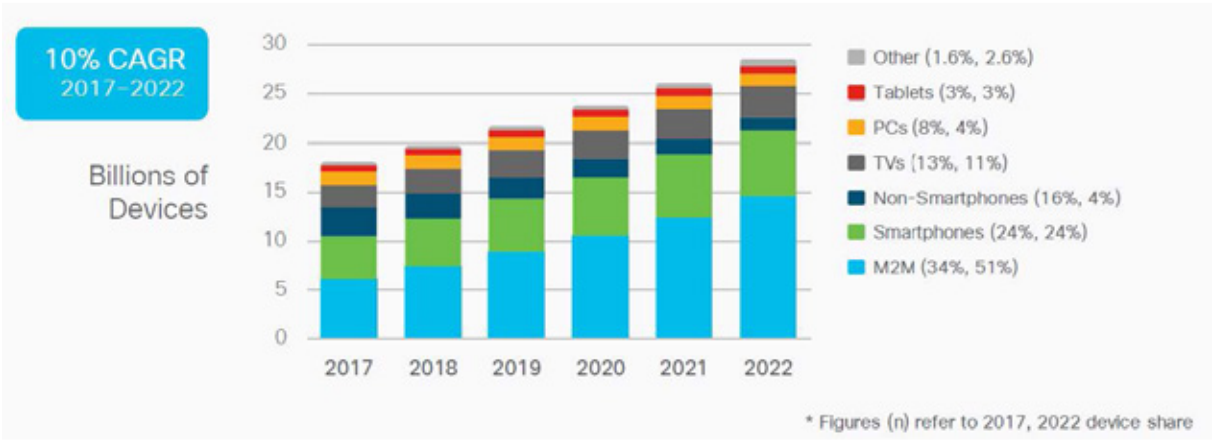
É inegável que os avanços tecnológicos vivenciados nas últimas décadas, especialmente os relacionados às comunicações e ao surgimento da Internet, transformaram o modo como as pessoas se relacionam entre si e com o próprio meio em que estão inseridas, sendo perceptíveis as inúmeras facilidades que surgiram a partir disso.

A possibilidade de comunicação instantânea entre pessoas de quaisquer lugares do mundo, independentemente da distância entre elas; o trânsito ágil pelas cidades por meio de mapas digitais interativos, que apontam rotas, restaurantes e pontos turísticos; os serviços online de cadastro e resolução de problemas que dispensam a necessidade de deslocamentos; o compartilhamento de notícias e opiniões por meio das redes sociais, e várias outras atividades da realidade se tornaram mais eficientes e simplificadas.

Contudo, essa intensa troca de informação tem resultado em um enorme acúmulo e intercâmbio de dados pessoais por um incontável número de empresas e pessoas físicas, muitas vezes de forma não consentida, ou mesmo não percebida pelos titulares dessas informações, movimentando um verdadeiro mercado em que os dados pessoais são a nova moeda de troca. E as estimativas apontam que esse é apenas o início de um inevitável processo, de proporções extraordinárias, cujas consequências, em diversos aspectos, ainda não podem ser antecipadas em sua totalidade.

Em seu último relatório de tendências, atualizado em 27/02/2019, a companhia Cisco, uma das maiores e mais relevantes empresas de tecnologia do mundo, previu que, em 2022, o número de dispositivos conectados será superior a três vezes o tamanho da população mundial (3,6 dispositivos por pessoa), atingindo 28,5 bilhões, como ilustrado na Figura 1 a seguir: abertura à consensualidade. Foi examinada, ainda, a dicotomia imperatividade-consensualidade, bem como as prerrogativas da atuação imperativa e os pressupostos teóricos da consensualidade.

Figura 1: Previsão de crescimento mundial de dispositivos conectados 2017-2022



Fonte: CISCO, 2019

É evidente, portanto, que a exposição a diferentes fontes de coleta de dados, bem como a possibilidade de acesso a essas informações por terceiros, já experimentadas pelos indivíduos nos dias atuais, alcançará patamares nunca antes vivenciados.

Nesse sentido, a temática da proteção da privacidade dos indivíduos emerge como fator de extrema relevância para as sociedades presentes e futuras. Sendo assim, o debate acerca dos limites a serem resguardados e das consequências da falta de controle e do uso mal intencionado de dados pessoais vem assumindo um papel de protagonismo no contexto da IoT.

Ao redor do mundo, o tema tem sido objeto de atenção não só pelo Governo ou pelas pessoas em geral, mas também por empresas na esfera privada, como revela a 22ª Pesquisa Anual Global com CEOs da PricewaterhouseCoopers – PwC[1], publicada em 2019:

> "Este ano, há mais nuances na discussão. Preocupações relacionadas à tecnologia estão crescendo e os líderes estão aprendendo como alavancar tecnologias avançadas de maneira responsável e sustentável, com o olhar cada vez mais crítico sobre questões como segurança cibernética e privacidade, propriedade de dados e integridade" (tradução livre, grifo nosso)

É, portanto, crucial que, também no Brasil, seja dada a devida relevância ao tema e que sejam efetivamente postos em evidência os riscos e as consequências advindas dessa nova realidade, para que todos tenham ciência do alcance e do poder de influência na vida das pessoas que surge a partir do uso de informações pessoais por parte de entes privados e governamentais.

1 https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf

Há que se promover um debate claro e transparente, que seja compreendido por todos os cidadãos, de modo a estabelecer mecanismos de proteção e controle do armazenamento, da utilização e do repasse dessas informações, no intuito de salvaguardar a vida privada, a segurança, a liberdade e o direito à privacidade dos usuários dos serviços.

O presente artigo de conclusão de especialização se propõe a expor uma visão geral sobre a Internet das Coisas e abordar alguns aspectos específicos relacionados à necessidade de proteção da privacidade no contexto da evolução da IoT, elucidando debates sobre o tema e listando alguns pontos sensíveis sobre o acesso a dados pessoais e sua respectiva utilização. Considerando-se a extensa literatura internacional e a, ainda, relativamente escassa produção brasileiras, busca-se contribuir para um entendimento mais estruturado do assunto.

São apresentadas algumas referências mundiais acerca da proteção da privacidade, para demonstrar a forma como o tema vem sendo tratado em outros países do mundo e, por fim, abordam-se alguns aspectos da recém-publicada Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais brasileira (LGPD), e das alterações posteriormente introduzidas pela Medida Provisória nº 869/2018.

Considerando-se que o assunto vem sendo mais amplamente debatido somente nos últimos anos, a metodologia adotada consistiu na análise de artigos científicos produzidos em instituições acadêmicas, bem como reportagens, documentos governamentais e estudos divulgados na mídia especializada ou por empresas do setor, em sua grande maioria em língua inglesa. As traduções presentes neste artigo foram feitas de modo livre.

2. O que é a Internet das Coisas?

Não há uma definição única e exata para a Internet das Coisas. Na verdade, o termo é frequentemente utilizado de forma genérica para se referir à multiplicação de objetos nas casas, ambientes de trabalho, cidades e indústrias que vêm sendo conectados à Internet e adquirindo diversos níveis de inteligência e capacidade de processamento. Em sentido amplo, portanto, trata-se não apenas de conectar coisas, mas também de dotá-las do poder de processar dados, tornando-as “inteligentes”.

Assim, a IoT (*Internet of Things*) se refere à crescente emergência de dispositivos, muitas vezes ordinários, desempenhando funções diferentes das que usualmente executaram (ROSNER; KENNEALLY, 2018): geladeiras que se comunicam diretamente com mercados e solicitam a reposição de produtos sem a necessidade de intervenção de seus donos, carros que dirigem sozinhos pelas ruas a um determinado destino, prédios que sabem onde estão localizadas todas as pessoas em seu interior e são

capazes de analisar e controlar diferentes parâmetros estruturais e de ambientação, são alguns exemplos.

A origem do termo, contudo, remonta a 1999, quando o então diretor do Auto-ID Center do MIT[2], Kevin Ashton, utilizou a expressão como título de uma apresentação feita na empresa Procter & Gamble (P&G). Já naquela época, como expõe o próprio autor (ASHTON, 2009), sua visão era a de que os computadores e, consequentemente, a Internet eram quase totalmente dependentes de ideias e informações providas e criadas por seres humanos, que, por sua própria natureza, detinham atenção, tempo e acurácia limitados, não sendo totalmente capazes de capturar dados sobre as coisas no mundo real. Esse era um importante aspecto a ser considerado, tendo em vista que os seres humanos e o meio ambiente eram físicos – existiam de fato – e, portanto, a economia, a sociedade e a própria subsistência das pessoas não se baseavam em ideias, mas sim em "coisas".

Ideias e informações eram importantes, mas, segundo Kevin, coisas eram muito mais. Contudo, ainda assim, a tecnologia da informação era tão dependente dos dados originados por pessoas que os computadores sabiam mais sobre ideias que sobre coisas. Nesse sentido, o autor afirmava que, se tivéssemos computadores capazes de saber tudo sobre as coisas, por meio de dados colhidos sem a ajuda de pessoas, seria possível rastrear e contabilizar qualquer elemento, reduzindo desperdícios, perdas e custos; identificar a necessidade de reposição, reparo ou substituição de itens; ou verificar as condições de armazenamento de itens perecíveis.

Assim, ao cunhar o termo "Internet das Coisas", Kevin propunha capacitar os computadores a colherem informações por conta própria, para que pudessem "ver, ouvir e sentir" o mundo sozinhos. Os sensores e as tecnologias de radiofrequência permitiriam isso: identificar, observar e entender o mundo sem as limitações do fornecimento de dados por seres humanos, tendo a IoT, desse modo, o potencial de mudar o mundo como a própria Internet mudou, ou até mais.

Vale destacar, contudo, que embora o termo tenha surgido em 1999, a ideia de objetos não computacionais conectados em rede surgiu bem antes. Como expõe Dr. Gilad Rosner (2016), já em 1970, programadores da *Carnegie Mellon University* conectaram uma máquina de Coca-Cola à Arpanet, predecessora da Internet. Nas décadas seguintes, vários conceitos, muitas vezes sobrepostos, surgiram para descrever um mundo em que objetos conversariam entre si, monitorando silenciosamente máquinas, ambientes e seres humanos por meio de sensores: inteligência ambiental (*ambient intelligence*), contexto computacional (*contextual computing*), computação ubíqua

2 Fundado em 1999, o Auto-ID Center foi uma parceria única entre aproximadamente cem companhias multinacionais e sete das principais universidades de pesquisa do mundo, visando ao desenvolvimento de padrões e ao desenho da infraestrutura necessária para criar uma "Internet das Coisas" (http://www.autoidlabs.org.uk/).

(*ubiquitous computing*), *machine-to-machine* (M2M) e, mais recentemente, sistemas ciber-físicos (*cyber-physical systems*).

Também o conceito de conectar máquinas a computadores não é novo: nas fábricas, por exemplo, sistemas computadorizados de controle industrial (ICS) e Sistemas de Supervisão e Aquisição de Dados (SCADA) há tempos já controlavam, monitoravam e ajustavam a operação de máquinas industriais, com base em suas condições operacionais (NSTAC, 2014).

Contudo, como assevera o Comitê Nacional Consultivo de Segurança das Telecomunicações dos EUA (*National Security Telecommunications Advisory Committee* – NSTAC)[3], o que diferencia a Internet das Coisas dos demais avanços históricos em tecnologia da informação é seu explosivo crescimento com base em três dimensões principais: escalabilidade em ritmo nunca antes visto; amplo escopo de desenvolvimento, que abrange desde de sistemas e indústrias complexos a dispositivos bastante simples; e rápida incorporação em todas as áreas de infraestrutura.

Assim, a IoT reúne várias tendências convergentes, como o generalizado acesso às telecomunicações e redes locais a baixo custo, sensores mais baratos e precisos, maior capacidade de processamento, miniaturização e nanotecnologia, tecnologias de rastreamento de localização (como o GPS), criação de protótipos a baixo custo e a adoção generalizada dos smartfones como uma plataforma para a interface de dispositivos. Esses avanços tecnológicos congruentes fizeram com que a IoT ultrapassasse os anteriores, permitindo que ela saísse do ambiente confinado dos computadores e se conectasse diretamente com o mundo físico, ou "das coisas" (NSTAC, 2014).

De forma um pouco mais sistematizada, a União Internacional das Telecomunicações[4], define a Internet das Coisas como uma infraestrutura global para a sociedade da informação, que viabiliza serviços avançados por meio da interconexão de coisas (físicas e virtuais), com base na interoperabilidade das Tecnologias da Informação e Comunicação (TIC), em constante evolução (UIT, 2012).

Ainda dentro desse conceito, de acordo com o NSTAC, pode-se dizer que os dispositivos relacionados à IoT geralmente compartilham três características: (1) são objetos comuns individualizados em uma rede, podendo ser endereçados; (2) esses

3 Há mais de 30 anos, a NSTAC reúne executivos das principais empresas de telecomunicações, tecnologia da informação, finanças e da indústria aeroespacial, com o objetivo de desenvolver recomendações ao Presidente dos Estados Unidos que assegurem conexões essenciais de telecomunicações em qualquer evento ou crise e ajudem o governo norte-americano a manter uma postura de comunicação nacional confiável, segura e resiliente (https://www.dhs.gov/about-nstac).

4 A UIT é a agência do Sistema das Nações Unidas dedicada a temas relacionados às Tecnologias da Informação e Comunicação (TICs), fundada em 1865 (https://nacoesunidas.org/agencia/uit/).

objetos físicos estão interconectados; e (3) são inteligentes, podendo desempenhar funções adaptativas, sozinhos ou em colaboração com outros dispositivos e aplicações, baseados em programações e dados coletados do mundo físico.

De todas as várias tentativas de se definir a Internet das Coisas, uma expressão parece prevalecer em todas elas, que são "dispositivos conectados". Nesse sentido, Dr. Gilad Rosner (2016) expõe que o foco deixou de estar voltado somente à produção de computadores genéricos, que desempenham inúmeras funções (como os desktops, laptops e até mesmo os smartfones), e passou ao desenvolvimento de dispositivos, no sentido de se tratarem de objetos que não são desenhados para serem completos ou genéricos, mas para desempenhar um número específico de funções. Isto é, carros, drones, televisões, brinquedos, aparelhos com fins médicos ou voltados a atividades físicas certamente dispõem de capacidade de processamento, mas eles são primeiro "coisas" e, segundo, computadores.

Em suma, o mesmo autor expressa que a IoT é um título para uma variedade de definições, tecnologias e tendências, e que – embora a ideia de conectar dispositivos não seja nova – políticos, jornalistas e o público em geral têm se voltado para esse tema somente agora, em virtude de esses dispositivos estarem começando a se popularizar e a invadir a vida pessoal de uma forma que os desktops e laptops não fizeram. Dr. Gilad R. ainda prediz que o termo "Internet das Coisas", em algum momento, desaparecerá, conforme essa realidade se torne efetivamente parte do cotidiano de todos.

3. Como as "coisas" se tornam inteligentes?

Como visto, a Internet das Coisas vai além da simples conexão de máquinas e equipamentos à Internet, referindo-se, na verdade, ao surgimento de uma rede mundial de dispositivos interconectados e interdependentes, com capacidade de capturar e processar dados do mundo físico para produzir informação com elevada acurácia e em grande quantidade no mundo digital, bem como induzir adaptações e ações que tornem as operações mais eficientes, contribuindo com o desempenho de atividades nos mais diversos ramos de atuação humana.

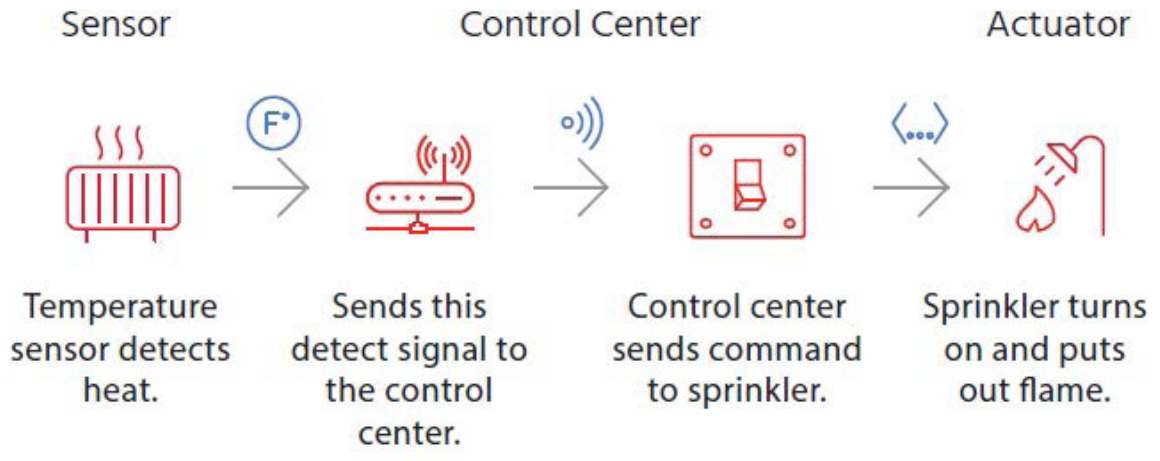
As "coisas", na Internet das Coisas, incluem potencialmente tudo – seres vivos, postes de luz, fábricas, sprinklers de jardim, automóveis, foguetes, barragens. Embora esses dispositivos sejam caracterizados como "inteligentes", são, na verdade, os sensores, microcontroladores e atuadores incluídos nesses dispositivos os responsáveis, respectivamente, por coletar, processar os dados e receber instruções pela Internet, fazendo as coisas agirem (CURTIN UNIVERSITY, 2019). Daí a capacidade de "sentir e agir" das coisas.

Considerando-se que a inteligência e o valor de um sistema de IoT são, em grande medida, baseados no que pode ser extraído dos dados a ele associados, os sensores são parte fundamental da IoT, pois conseguem capturar os parâmetros do mundo físico. Com base nas inovações em termos de materiais e nanotecnologia, os sensores vêm evoluindo amplamente, resultando em maior acurácia, menores custos e tamanhos, e na capacidade de detectar e medir parâmetros antes impossíveis (BRIDGERA; RIOT, 2017).

Em linhas gerais, pode-se dizer que sensores são transdutores, ou seja, componentes capazes de converter uma forma de energia em outra. Então, no caso de um sensor, o transdutor converte um fenômeno físico em um impulso elétrico que pode ser interpretado. De forma análoga, os atuadores são também transdutores que operam no sentido inverso ao dos sensores, transformando um sinal elétrico de entrada em uma ação.

Assim, em um sistema de IoT típico, o sensor coleta dados e os encaminha a um centro de controle que, por sua vez, processa uma decisão e envia o respectivo comando de volta ao atuador, em resposta à variável de entrada captada pelo sensor. A Figura 2 ilustra o funcionamento de um sprinkler ao detectar a presença de calor em determinado ambiente.

Figura 2: Esquema simplificador de acionamento de um sprinkler



Fonte: BRIDGERA; RIOT, 2017.

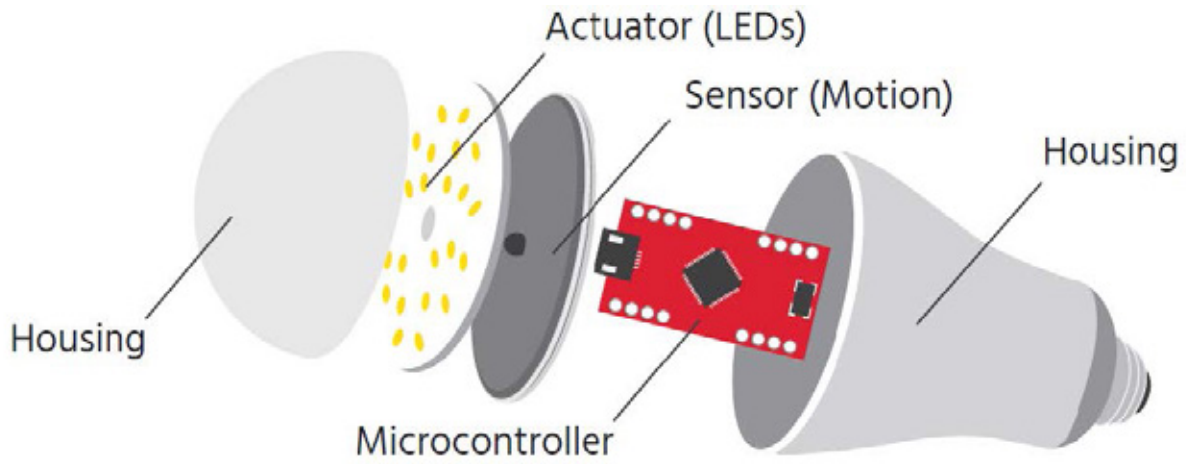
Existem diversos tipos de sensores: de corrente elétrica, tensão elétrica, som, temperatura, calor, presença, umidade, movimento, entre muitos outros. Da mesma forma, existem múltiplas formas de se medir determinado fenômeno, a depender da aplicação desejada, que darão origem a diferentes bases de dados a partir de uma mesma realidade observada.

Quanto ao sistema de controle, em IoT, os dispositivos necessitam basicamente de dois componentes: “cérebro” e conectividade. Normalmente, como descrito no livro

A Reference Guide to the Internet of Things (2017), os dispositivos usam um microcontrolador como "cérebro", que dispõe de um microprocessador, memória e portas de entrada e saída. As funções desejadas e o tamanho do dispositivo determinarão a capacidade e as proporções do microcontrolador.

A conectividade, por sua vez, é necessária para a comunicação com um elemento remoto de controle ou com a Internet. A forma como ela será provida variará de acordo com a localização, o ambiente e o tipo de dispositivo em questão. A Figura 3 exemplifica uma lâmpada de LED ativada por meio de um sensor de movimento, no intuito de ilustrar os três componentes (sensor, atuador e microcontrolador) em funcionamento em um dispositivo simples:

Figura 3: Sensor, atuador e microcontrolador em uma lâmpada de LED



Fonte: BRIDGERA; RIOT, 2017.

4. Privacidade e a IoT

4.1 4.1 O que é Privacidade?

De modo semelhante à Internet das Coisas, também o conceito de privacidade não é algo estanque ou simples de ser estabelecido. É um fenômeno econômico, político, legal, social e cultural, que varia segundo o país, a região, a sociedade e suas tradições culturais e legais.

Um marco de destaque na discussão contemporânea sobre o tema data de 1890, quando Warren e Brandeis, teóricos americanos, publicaram um artigo na *Harvard Law*

Review, intitulado *The Right to Privacy* (O Direito à Privacidade, em português), colocando em evidência "a ocorrência de transformações sociais, políticas e econômicas, bem como o surgimento de novos inventos, como a fotografia, que contribuíram para a ocorrência de violações da vida privada das pessoas" (ZANINI, 2015).

A partir dessa publicação, o direito à privacidade, ou "o direito de ser deixado só" (*the right to be let alone*), passou efetivamente a ganhar relevo nas discussões jurídicas, como um princípio civil relevante da sociedade.

Embora o artigo, considerado a obra fundamental sobre o tema, permaneça ainda bastante atual, é inegável que o conceito evoluiu desde então, indo muito além da simples prerrogativa de ser "deixado só".

Já em 1967, Alan Westin, estudioso americano, definiu a privacidade como "a reivindicação de indivíduos, grupos ou instituições de determinarem, por si mesmos, quando, como e em que medida informações sobre eles podem ser divulgadas a outros"[5]. Ou seja, já nessa época, passou-se a observar a privacidade na perspectiva do controle do indivíduo sobre o uso de suas informações pessoais por terceiros.

Na mesma década, em 1960, William Prosser (apud ROSNER, 2016), estudioso do direito americano, havia identificado quatro tipos de atividades prejudiciais, que o direito à privacidade buscava dissuadir: intromissão na reclusão de alguém, ou em seus relacionamentos pessoais; divulgação pública de fatos privados constrangedores; divulgação de informações falsas sobre determinada pessoa, difamação; e utilização do nome ou imagem de alguém sem a sua permissão; falsidade ideológica.

Apesar de esses conceitos já se apresentarem mais amplos, eles têm como centro de observação a pessoa e os prejuízos que podem recair sobre ela. A privacidade, contudo, deve ser observada também sob a óptica da sociedade, sendo vital para o seu funcionamento e para a democracia (ROSNER, 2016).

O direito à privacidade e à proteção dos dados é essencial para garantir a participação imparcial dos cidadãos na vida política, bem como a liberdade de expressão, de modo que ele não visa apenas à proteção do indivíduo, mas também à manutenção de um verdadeiro estado democrático de direito.

Nesse sentido, a privacidade "promove e encoraja a autonomia moral dos cidadãos, pilar central da democracia" (GAVISON, 1980). Sua tutela deve, portanto, ser vista como primordial ao interesse público, sendo fundamental que se promovam debates abertos e intensos acerca do tema e sua regulação e proteção pelo Estado.

---

5 "*The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*" (Westin, A. 1967. *Privacy and Freedom*. New York: Atheneum apud ROSNER, 2016).

Adicionalmente, não se pode ignorar que, também ao Estado, devem-se impor limites relativos ao respeito à privacidade de cada cidadão, devendo haver regras específicas relacionadas à coleta de dados pessoais, ao monitoramento de pessoas, e outros aspectos igualmente relevantes.

Dando seguimento ao trabalho iniciado por W. Prosser, Daniel Solove (2016, p. 477), professor americano citado por Dr. Gilad R. (2016), formulou uma taxonomia da privacidade, no intuito de retirar o foco da busca pela definição do que seria a privacidade, para colocá-lo nas ações que afetassem a privacidade de um indivíduo, resumidamente exposta na Tabela 1.

Tabela 1: Taxonomia da privacidade por Daniel Solove

Coleta de informações	Monitoramento: observar, ouvir ou gravar as atividades de um indivíduo Questionamento: interrogar ou sondar informações
Processamento de informações	**Agregação:** combinar dados de diversas fontes sobre uma mesma pessoa **Identificação:** relacionar ou ligar informações a um determinado indivíduo **Insegurança:** falta de cuidado na proteção de informações armazenadas **Uso secundário:** utilizar informações para fins diferentes dos originalmente acordados, sem o consentimento do titular das informações **Exclusão:** não permitir que o indivíduo tenha conhecimento dos dados que outros dispõem sobre ele, nem que participe das decisões acerca do uso e tratamento desses dados.
Disseminação de informações	**Quebra de confidencialidade:** quebrar a promessa de que as informações sobre alguém permaneceriam confidenciais **Divulgação:** revelar informações que afetam a imagem de alguém **Exposição:** expor o corpo ou o sofrimento de alguém **Acessibilidade excessiva:** ampliar o acesso às informações sobre alguém **Chantagem:** ameaçar alguém em troca de não revelar alguma informação pessoal **Apropriação:** utilizar a identidade de alguém para o interesse de outrem
Distorção	**Disseminar** informações falsas ou enganosas sobre uma pessoa
Invasão	**Intromissão:** invadir a tranquilidade ou a reclusão de outra pessoa **Interferência**: atacar e interferir na vida amorosa de outra pessoa

Fonte: ROSNER, 2016.

Rosner destaca que, embora essa classificação foque no indivíduo, deve-se compreender que perdas no campo da privacidade pessoal geram prejuízos à sociedade como um todo. Por exemplo, uma pessoa que sinta que suas comunicações estejam sendo monitoradas, ou que ela esteja sendo vigiada, tende a deixar de exprimir opini-

ões que possam ser entendidas como desvios a normas estabelecidas, gerando uma homogeneização de discursos contrária à democracia e à liberdade, que se baseiam no respeito a diferentes pontos de vista. “Discórdia, opiniões impopulares e embates intelectuais são componentes essenciais de uma sociedade livre, e a privacidade ajuda a protegê-los”.

Ainda, é necessário lembrar que a preservação da privacidade custa dinheiro, de modo que esses dois fatores não podem ser dissociados. Com isso, as empresas precisam de uma justificativa econômica para incorporar a proteção da privacidade em seus negócios, que pode vir de normas regulatórias, questões comerciais (diferencial concorrencial), aderência às melhores práticas, obrigações contratuais, proteção da marca, receio de processos judiciais, entre outros.

Por fim, o autor destaca que, muito embora os campos da segurança e da privacidade sejam confundidos, eles não são a mesma coisa. A privacidade depende tecnologicamente da segurança, mas eles são aspectos distintos. A segurança da informação é normalmente definida por meio dos atributos da integridade (salvaguardar os dados contra modificações indesejadas), confidencialidade (assegurar que as informações sejam acessadas apenas por pessoas autorizadas) e disponibilidade (garantir que os dados estejam disponíveis quando requeridos pelo usuário).

Embora a confidencialidade mantenha uma relação direta com a privacidade, a segurança dos dados, de forma geral, diz respeito a garantir que os sistemas funcionem conforme projetado e que sejam acessados apenas por pessoas autorizadas.

Dr. Gilad R. exemplifica essa diferença por meio de um caso real, ocorrido em 2015, em que hackers foram capazes de acessar o sistema de som *bluetooth* de automóveis da marca Jeep, para remotamente desligar os motores do carro e acionar os freios com o veículo em movimento. O ocorrido representou uma falha de segurança. A definição de quem poderia acessar as informações armazenadas pelo carro, sua localização, quem esteve no automóvel, por onde andou, representa questões relacionadas à privacidade, que se relacionam ao fluxo da informação, à exposição dos dados e à identificação de pessoas autorizadas.

4.2 Riscos à Privacidade na IoT

As inovações e facilidades introduzidas pela intensa propagação de dispositivos conectados, presenciada nas últimas décadas, trazem também consigo novos desafios, que já são percebidos em diferentes aspectos da sociedade.

Nessa nova realidade, em que centenas de objetos inteligentes passam a participar ativamente do cotidiano de cada pessoa – muitas vezes, sem o seu conhecimento ou

consentimento –, é impossível não se pensar sobre os riscos e impactos à privacidade gerados por essas novas tecnologias que, a bem da verdade, vieram para ficar.

Pesquisadores e estudiosos do assunto vêm, há alguns anos, analisando os perigos associados à IoT no campo da privacidade. Dr. Gilad Rosner, consultor do governo britânico sobre o tema e fundador do IoT Privacy Forum, no livro Privacy and the Internet of Things ("Privacidade e a Internet das Coisas"), lista seis desses riscos, resumidamente detalhados a seguir:

4.2.1 Monitoramento intensificado

Um dos maiores riscos à privacidade que surge a partir de um mundo intensamente conectado por dispositivos capazes de coletar e processar dados é o elevado monitoramento das atividades e do cotidiano das pessoas.

Interessante notar que a capacidade de entender o contexto no qual os indivíduos estão inseridos, por meio da coleta de dados de áudio, vídeo, localização e outras formas de detecção, é um dos grandes pilares da IoT. São vastas as possibilidades de provimento de novos e importantes serviços que surgem a partir dessa coleta de informações, que inquestionavelmente aprimoraram as experiências dos usuários, possibilitam ganhos de eficiência, ampliam a segurança dos cidadãos, entre outros inúmeros benefícios.

Contudo, no campo da privacidade, as implicações são igualmente relevantes, considerando-se que os indivíduos estarão sendo constantemente observadas por máquinas e dispositivos que não podem controlar.

Como assevera Dr. Gilad, o monitoramento de atividades e pessoas não é algo recente, já existindo em diversas formas, como câmeras públicas de segurança e controle de localização pelos celulares. Na Internet das Coisas, entretanto, a grande questão passa a ser a proporção que essa capacidade de monitoramento atingirá, ramificando-se para aspectos que vão muito além da simples identificação de quem esteve presente em determinado local.

Há uma gama de informações pessoais que podem ser obtidas a partir de dados de localização, como hábitos esportivos (ou a ausência deles), orientação religiosa, visitas a clínicas médicas, presença em manifestações políticas, preferências de diversão e lazer, e uma série de outros hábitos que muitas vezes não se deseja divulgar.

Com a IoT, essas informações serão, cada vez mais, capturadas por dispositivos discretos e pouco invasivos, de modo que as pessoas muitas vezes não saberão que estão sendo vigiadas, nem para onde estão indo essas informações. "Ou seja, mais

dispositivos – e, portanto, mais organizações e sistemas – saberão em que lugar você está, em que lugar esteve, e, cada vez mais, para onde está indo" (ROSNER, 2016, tradução livre).

4.2.2 Coleta não consentida de dados

A introdução de dispositivos sensíveis no cotidiano das pessoas levanta questões relacionadas à temática do consentimento, visto sobre duas ópticas principais: o conhecimento de que dados pessoais de qualquer natureza estão sendo coletados, tanto em ambientes públicos, quanto privados; e a possibilidade de autorizar, ou coibir que essas informações sejam capturadas e compartilhadas.

Considerando-se que a IoT pode ser vista como uma estratégia de desenvolvimento de produtos, por meio da incorporação de crescente monitoramento, computação e conectividade em linhas de produção existentes (GILAD, 2016), o tratamento dessas questões engloba aspectos relacionados ao design dos produtos e também à autonomia dos usuários.

Estratégias comumente observadas na comercialização de diversos produtos e serviços, baseadas em contratos de adesão ou manifestação de acordo com termos de uso, deixam pouca, ou nenhuma, opção ao indivíduo acerca do que ele de fato deseja fazer com seus dados, reduzindo sua capacidade de consentimento. Por exemplo, em um carro que constantemente rastreie sua posição, deve existir a possibilidade de que o condutor desabilite essa funcionalidade por completo? De outra forma, deve existir uma constante manifestação de consentimento sobre toda a informação coletada e transmitida sobre um indivíduo?

Outro ponto a ser destacado relaciona-se à proteção de dados pessoais de crianças e adolescentes. Considerando-se sua capacidade limitada de avaliar riscos e consequências, é necessário que disponham de regras de proteção específicas no que concerne à coleta, transmissão e uso dessas informações, inclusive para fins comerciais.

4.2.3 Armazenamento de informações médicas

Em diversos países do mundo, entre eles o Brasil, a guarda de informações médicas de diferentes fontes relacionadas a um determinado indivíduo é regida por um conjunto específico de regras, voltadas a sua proteção. Esses dados recebem tratamento sigiloso, sendo sua divulgação permitida em casos bastante específicos[6].

6 https://www.cremesp.org.br/?siteAcao=Publicacoes&acao=detalhes_capitulos&cod_capitulo=57

As razões para que esses dados mereçam esse tratamento diferenciado envolvem a necessária garantia ao paciente de que suas informações não serão reveladas sem o seu consentimento, gerando uma relação de confiança e transparência; a proteção contra a estigmatização, perda de emprego, ou qualquer outro dano que possa ser gerado a partir da revelação de uma condição médica ou doença; a crença de as pessoas detenham o controle sobre quem deve ter conhecimento sobre sua condição física ou mental (GILAD, 2016).

Embora exista todo um arcabouço de normas destinadas à regulação dos dados médicos, com a IoT, deixa-se de ter uma divisão clara acerca do que é considerado informação médica, além de também não se ter mais uma visão estrita da cadeia de geração e transmissão dessas informações, com a introdução de novos stakeholders e novas tecnologias.

A partir de dispositivos comuns (como um relógio, por exemplo) que, já nos dias atuais, detectam e armazenam batimentos cardíacos, pressão sanguínea, padrões de sono, contam calorias, entre outros parâmetros biométricos, surge a dúvida se esses dados se distinguem de informações médicas, essas protegidas por sigilo.

As consequências desse limiar ainda não bem traçado, que se refletem no tratamento regulatório dessas informações, são bem resumidas pelo Dr. Heather Patterson, especialista na avaliação da privacidade em dispositivos médicos móveis:

> "Forças convergentes de cunho tecnológico, regulatório e social, apontam para um futuro de crescente decisões de saúde personalizadas, guiadas por dados e colaborativas. **Um dos grandes protagonistas dessa transição é a disponibilidade imediata de sensores e aplicativos comerciais, de prateleira, com baixo custo, que permitem aos indivíduos comunicar uma ampla gama atributos comportamentais e fisiológicos em tempo real**. (...)
>
> A escala, o escopo e o fluxo não tradicional de informações médicas, em conjunto com técnicas sofisticadas de mineração de dados que dão suporte a inferências confiáveis, **colocam os consumidores em uma posição vulnerável a constrangimentos e danos à reputação; à discriminação por empregadores e seguradoras; e a comportamentos comerciais e publicitários indesejados**" (PATTERSON, 2013, tradução livre, grifo nosso)

O compartilhamento não consentido dessas informações, que demonstra a interdependência dos temas, torna ainda mais relevante que se discuta o adequado tratamento desses dados em termos regulatórios.

A título de exemplo, uma pesquisa conduzida em 2013, sobre 23 aplicativos gratuitos e 20 pagos ligados a saúde e esporte, detectou que 39% dos gratuitos e 30% dos aplicativos pagos compartilhavam informações com alguma entidade não discriminada no aplicativo ou na política de privacidade, e que 26% dos gratuitos e 40% dos pagos sequer tinham uma política de privacidade (ACKERMAN, 2013). É notório o risco a que os indivíduos se submetem, muitas vezes de forma desavisada.

Dr. Gilad ressalta uma das grandes preocupações da coleta e compartilhamento dessas informações como sendo o seu uso inapropriado por seguradoras contra seus clientes, em processos litigiosos.

4.2.4 Quebra da segregação de contextos informacionais

De todos os riscos anteriormente mencionados, destacados pelo autor, é impossível não observar a nova realidade trazida pela Internet das Coisas, que surge da mistura de dados de diferentes fontes e aspectos da vida das pessoas, descrito pela expressão "fusão de sensores" (*sensor fusion*).

Em IoT, a expressão refere-se ao fato de que a combinação de dois ou mais sensores ou dispositivos pode gerar inferências inesperadas acerca de diferentes aspectos, muitas vezes sem qualquer relação com o propósito ou contexto originalmente imaginado para esses sensores.

Nesse sentido, a quebra da segregação de contextos informacionais surge como uma consequência dessa fusão de sensores e da tendência ao compartilhamento de dados entre múltiplos contextos – saúde, trabalho, educação, finanças, e outros. Ou seja, informações de variados assuntos, ambientes e circunstâncias sendo compartilhadas em diferentes contextos, gerando novas informações acerca de um indivíduo. Considerando-se que cada informação é adequada para um determinado contexto e circunstância, o desrespeito a esses limites é sentido pelas pessoas como uma violação da sua privacidade.

Por exemplo, é adequado que um médico compartilhe informações sobre a saúde de um paciente com um laboratório, mas não que as encaminhe à área de recursos humanos de uma empresa. Da mesma forma, é coerente que alguém compartilhe suas informações financeiras com um contador, mas não se mostra coerente que essas informações sejam enviadas sem consentimento ao setor de crédito de um banco.

É notória a importância de que sejam debatidas as questões relacionadas à segregação de contextos na realidade da IoT. As discussões modernas caminham no sentido de estabelecer que o contexto importa; isto é, na regulação do tratamento das infor-

mações há que se considerar quais dados são capturados; como, onde e com quem são compartilhados.

Na Alemanha, por exemplo, a corte constitucional determinou que o Estado não pode agir como um grande banco de dados, coletando e processando dados de um contexto para outro. Nos Estados Unidos, desde 2012, há normas que caminham no sentido de estabelecer como direito do consumidor esperar que as companhias coletes, usem e compartilhem informações pessoais em condições coerentes com o contexto no qual o consumidor forneceu esses dados.

4.2.5 Diversificação de partes interessadas (stakeholders)

O risco de diversificação de partes interessadas elencado por Dr. Gilad refere-se ao aumento de *stakeholders* em toda a cadeia de manufatura, coleta, processamento, transmissão de dados. O autor destaca não apenas seu incremento em termos quantitativos, mas também em termos qualitativos.

A Internet das Coisas ampliou, em grande medida, a possibilidade de que novos participantes, muitas vezes com pouca ou nenhuma experiência, passem a atuar no mercado e ter acesso a um elevado volume de dados.

Embora as grandes empresas, tradicionais no setor de manufatura de equipamentos eletrônicos (como Siemens, Intel, Cisco e outras), permaneçam atuando com grande força no desenvolvimento de novos dispositivos conectados, um incontável número de *startups*, empreendedores amadores e novas companhias têm se empenhado na criação do futuro das coisas conectadas.

E, apesar de haver inúmeros benefícios em termos de inovação, abertura de mercado e outros aspectos relevantes, há que se considerar que esses novos atores muitas vezes carecem de experiência e conhecimento acerca das práticas e regras relacionadas à segurança e à privacidade das informações. Além disso, para muitas dessas novas empresas, os custos afetos à gestão desses requisitos podem não ser a prioridade no momento de desenvolvimento das soluções.

Esse entendimento foi também manifestado em um artigo publicado no site da FTC (*Federal Trade Comission*), no qual o então *Chief Technologist*, Ashkan Soltani, expõe os motivos pelos quais a segurança em IoT é de grande importância. No presente tópico, dois desses itens se destacam:

> "3. Além do sistema operacional, os próprios chips e drivers incorporados aos dispositivos reúnem **muitos produtos diferentes, feitos por vários fabricantes de IoT, de modo que uma vulnerabilidade**

> **encontrada em um elemento pode ser explorada em uma classe maior de dispositivos**;
>
> 4. O crescimento e a diversidade de hardwares significam também que muitos dispositivos introduzidos no mercado de IoT serão fabricados **por novos entrantes com pouca experiência prévia em desenvolvimento e segurança de *softwares***" (SOLTANI, 2015, tradução livre, grifo nosso)

Soma-se a isso a cultura da retenção e acúmulo de informações, ainda que sem uma finalidade pré-estabelecida (coletam-se todos os dados possíveis, quer sejam usados, ou não), que vai de encontro a um dos princípios básicos da privacidade, qual seja restringir a coleta de informações ao mínimo necessário.

É como pensar na IoT como uma cadeia de suprimentos, em que os dados pessoais coletados de todos os indivíduos atuam como os insumos, que são coletados, transportados, enriquecidos, manipulados por interessados diretos, depois vendidos a terceiros e, eventualmente, retornados à fonte dos dados. Nesse processo, há diferentes intermediários: fabricantes de componentes eletrônicos, camadas de transporte de dados, redes de comunicação, servidores, analistas e consultores externos. (GILAD, 2016)

À medida que esse ecossistema de dispositivos conectados evolui, a cadeia vai se tornando mais longa e complexa, enquanto as fontes de dados também se multiplicam. O ponto crucial da diversificação de partes interessadas, então, reside em garantir que todos os participantes dessa cadeia atuem com honestidade no uso e compartilhamento de dados pessoais e que as preferências dos usuários sejam respeitadas.

4.2.6 Ampliação da vigilância governamental

Em 2013, as revelações de Edward Snowden, ex-analista contratado da NSA (Agência de Segurança Nacional dos Estados Unidos da América), tornando públicos diversos dados e informações secretas acerca do programa de monitoramento em massa do governo norteamericano, por meio da vigilância global de comunicações e tráfego de informações executada por meio de vários programas, expuseram ao mundo a extensa agenda de vigilância do país ao redor do mundo.

Gilad relembra que, de acordo com inúmeras matérias veiculadas por jornais como *The Guardian* e *The Washington Post*, um componente crítico que possibilitou esse extenso e profundo monitoramento de indivíduos de todo o planeta foi justamente o repasse de dados pessoais coletados por empresas privadas ao Governo norte-americano, tanto em função de pedidos diretos endereçados a essas companhias, quanto

por meio de espionagem e acesso não autorizado aos servidores de empresas como Google, Facebook, Apple e outras gigantes do mercado digital.

Em IoT, esse fato se torna de extrema relevância, considerando-se as estimativas referentes à avassaladora quantidade de informações pessoais coletadas de diversas fontes e por diferentes empresas em um futuro relativamente próximo. Em 2016, por exemplo, um exdiretor da inteligência norte-americana James Clapper afirmou ao Congresso que:

> "no futuro, os serviços de inteligência poderão utilizar [a Internet das Coisas] para identificação, vigilância, monitoramento, rastreamento e seleção para recrutamento, ou para ter acesso a redes e credenciais de usuários" (ACKERMAN; THIELMAN, 2016).

É evidente, portanto, a importância do debate acerca das leis, da governança e dos limites à penetração da IoT nos espaços privados, bem como dos métodos técnicos para a proteção da privacidade e salvaguarda dos limites ao monitoramento da vida privada dos cidadãos por parte das autoridades governamentais de todo o mundo.

4.3 Experiências internacionais de regulação

Diante das perspectivas de intensa propagação de dispositivos capazes de coletar e processar dados de todos os indivíduos, nos mais diversos ambientes e contextos, fornecendo informações a um número crescente de atores, as questões relacionadas à proteção da privacidade e ao papel do Estado nesse cenário ganham contornos bastante complexos.

É evidente que, como já destacado, o avanço da tecnologia e do monitoramento traz inúmeros benefícios à sociedade, e que há diversas possibilidades e opiniões sobre modelos regulatórios a serem adotados no intuito da proteção da privacidade dos indivíduos. Contudo, embora não se pretenda criar entraves que impossibilitem a evolução tecnológica, as vulnerabilidades atreladas a essas novas tecnologias e a necessária proteção da vida privada, da liberdade de expressão e da intimidade dos cidadãos não podem ser deixadas em segundo plano.

Nesse sentido, alguns países registram, já há alguns anos, progressos em termos de arranjos normativos e institucionais voltados a essa temática, sendo importante estudar as soluções por eles adotadas.

No presente artigo, portanto, serão brevemente descritas as experiências dos Estados Unidos e da União Europeia, que adotaram desenhos regulatórios relacionados à proteção de dados pessoais bastante distintos entre si; bem como o panorama geral da

América Latina, com destaque para o Uruguai, que tem se sobressaído no tratamento do tema na região.

Embora apresentem diferenças, os três modelos colocam o foco no consentimento do titular para a coleta, o tratamento e o uso de seus dados pessoais, estabelecendo também obrigações de transparência quanto ao esclarecimento de informações aos usuários, e concedem a eles o direito de acesso, retificação e eliminação de dados (BNDESa, 2017).

4.3.1 União Europeia

Relativamente ao arranjo institucional, a União Europeia conta hoje com diversas organizações oficiais voltadas à proteção de dados pessoais.

Como órgão de supervisão, o sistema europeu estabeleceu uma autoridade independente, especificamente destinada à proteção de dados pessoais, em respeito ao art. 8º da Carta de Direitos Fundamentais da União Europeia[7], que estabelece:

> "Artigo 8º Proteção de dados pessoais
>
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
>
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
>
> 3. **O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente**." (grifo nosso)

A partir dessa disposição, foi fundada, em 2004, a Autoridade Europeia para a Proteção de Dados (*European Data Protection Supervisor* – EDPS), entidade supervisora e consultiva independente, a quem compete supervisionar o processamento de dados pessoais pela administração da UE, visando assegurar o cumprimento das regras de privacidade; aconselhar as instituições e os órgãos da UE sobre todos os aspectos relacionados ao tratamento de dados pessoais e às políticas e legislação associadas; lidar com reclamações e conduzir investigações; trabalhar com as autoridades na-

7 https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:12016P/TXT

cionais dos Estados-membro para assegurar a consistência na proteção de dados; monitorar novas tecnologias que podem ter impacto na proteção de dados[8].

Antes disso, contudo, desde meados dos anos 90, a proteção de dados pessoais já vinha sendo regulamentada pelo Parlamento e pelo Conselho Europeu, por meio das Diretivas nº 95/46/CE[9] e nº 2002/58/CE, editadas em um primeiro esforço de uniformizar a legislação existente sobre o assunto nos seus Estados-membro.

Relativamente à estruturação institucional, o normativo editado em 1995, destinado à "proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", criou um Grupo de Trabalho ("Grupo de proteção das pessoas"), composto por representantes das autoridades de controle de proteção de dados de cada Estadomembro, da Comissão Europeia e, posteriormente, da EDPS, com competência para emitir recomendações, pareceres e outros documentos sobre o tema.

Esse normativo foi recentemente substituído pela Diretiva (EU) 2016/680, editada em abril de 2016, mas que passou a vigorar em maio de 2018. Denominada Regulação Geral de Proteção de Dados (General Data Protection Regulation – GDPR), surgiu da necessidade de modernizar as regras anteriores, frente à evolução tecnológica vivenciada nas últimas décadas[10].

As novas regras revelam inúmeros avanços na regulação do tratamento de dados pessoais dos cidadãos europeus, sendo referenciada como "uma das grandes conquistas dos últimos anos"[11]. Reportagem veiculada pela Empresa Brasileira de Comunicação (EBC) expôs, resumidamente, alguns pontos de destaque da nova diretiva, reproduzidos a seguir:

> "A GDPR se aplica a **qualquer tratamento de dados de pessoas residindo na União Europeia, mesmo no caso de empresas sediadas em outros países** (como a americana Apple ou a sul-coreana Samsung, por exemplo). Isso inclui firmas que oferecem bens e serviços na região ou monitoram comportamento de seus cidadãos.
>
> Para o tratamento dos dados, **é necessário obter consentimento do titular, em um pedido que deve ser apresentado de forma clara e**

8 https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

9 https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A31995L0046

10 https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

11 https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

> **acessível, garantindo também o direito ao usuário de revogá-lo**. A norma estabelece uma série de direitos aos cidadãos: acessar as informações que uma empresa tenha, corrigi-las e negar que elas sejam objeto de tratamento.
>
> A lei incluiu um item polêmico, denominado **'direito ao esquecimento': a possibilidade de o usuário solicitar a retirada de suas informações de uma plataforma (como o Google)**, devendo a empresa avaliar se o pleito não fere o interesse público. A norma também previu o direito de a pessoa não submeter suas informações a decisões automatizadas, como as linhas do tempo do Facebook ou a recomendação de vídeos do YouTube.
>
> As **empresas são submetidas a diversas exigências**. Precisam notificar usuários em caso de um vazamento que implique risco a eles. Devem informar se há dados sendo processados, como e para qual finalidade. E caso instadas ficam obrigadas a fornecer os dados do usuário em um formato que outras máquinas podem ler, instituindo uma espécie de 'portabilidade de dados'. Também têm de adotar medidas tecnológicas para garantir a proteção dos dados dos usuários.
>
> A regulação estabelece penalidades **como multas de até 20 milhões de euros ou de 4% do faturamento anual da empresa punida (o que for maior)**. Os valores a serem pagos variam de acordo com a gravidade da infração. Isso vale tanto para quem processa os dados quanto para quem controla, incluindo armazenamentos feitos na "nuvem" (serviços que permitem acesso remoto a informações por meio da conexão à internet)." (VALENTE, 2018, grifo nosso)

Nota-se a seriedade com que o assunto tem sido tratado na União Europeia, bem como o avançar das discussões nesse continente, impondo regras rígidas e punições àqueles que as desrespeitam. Vale mencionar que, com a vigência do novo normativo, o antigo grupo de trabalho criado nos anos 90 foi substituído pelo Comitê Europeu para a Proteção de Dados.

Além das instituições descritas, há também o *Data Protection Officer* (DPO), no âmbito da Comissão Europeia, responsável por assegurar, de forma independente, que essa comissão aplique corretamente a lei que protege os dados pessoais dos indivíduos, mantendo, inclusive, um registo público que explica todas as operações realizadas pela Comissão que envolvam o processamento de dados pessoais[12]. O DPO tem, ainda, o dever de cooperar com a EDPS e informar os departamentos da Comissão

12 https://ec.europa.eu/info/departments/data-protection-officer_en

Europeia que coletem dados pessoais e as pessoas titulares desses dados sobre seus respectivos direitos e obrigações.

Além desse caráter predominantemente regulatório da proteção dos dados pessoais na União Europeia, estabelecida por meio de normativos contendo as regras de proteção das informações e as autoridades responsáveis por sua aplicação, tanto no nível nacional quanto no supranacional, o modelo também abarca características de corregulação. Exemplo disso são as *Binding Corporate Rules* (BCRs), normas vinculantes advindas de entidades privadas, em que "empresas europeias e estrangeiras definem contratualmente regras para a proteção de dados pessoais em suas trocas transnacionais. Contudo, essas normas corporativas passam por processo de homologação perante a autoridade de proteção de dados de cada país envolvido na operação". A legislação implementada em 1995 já permitia que países-membros utilizassem esse tipo de abordagem na proteção de dados pessoais, prevendo a possibilidade de que cada país convidasse representantes de determinado setor para elaborar um conjunto de regras de conduta para o segmento, que poderia ser aprovado e obter força de legislação (BNDESa, 2017).

Indo ao encontro dessas práticas corregulatórias, também no novo regulamento, o tema das *Binding Corporate Rules* é tratado em artigo específico do texto (art. 47), que estabelece diversas regras e diretrizes para o adequado uso do instrumento.

4.3.2 Estados Unidos da América

Em abordagem absolutamente diferente, mas também de extrema relevância no panorama mundial, os Estados Unidos não possuem uma lei geral específica, de âmbito federal, que verse sobre a proteção dos dados pessoais dos indivíduos. Ao contrário, a matéria é regida por leis federais esparsas, leis estaduais, e códigos de conduta e regulamentos estipulados pelo setor privado (BNDESa, 2017), seguindo a lógica federativa do país.

As leis de âmbito federal são editadas para setores específicos, como: saúde e seguros (*Health Insurance Portability and Accountability Act* – HIPAA), bancário (*Gramm-LeachBliley Act* – GLB), telecomunicações (*Telecommunications Act*) e questões de consumo (*Children's Online Privacy Protection Act* – COPPA).

Além dessas, vale citar duas normas de cunho mais generalista: a Lei de Privacidade de Comunicação Eletrônica (ECPA, na sigla em inglês) que, entre outras coisas, proíbe a interceptação de mensagens telefônicas ou eletrônicas e estabelece mecanismos distintos de acesso a determinadas informações, especificando o que pode ser obtido somente por meio de ordem judicial ou mandado de busca. Ao longo dos anos, essa lei foi sendo atualizada para abranger também comunicações digitais. E a Lei de

Privacidade (*Privacy Act*) que estabelece as diretrizes para a coleta, armazenamento, uso e disseminação de dados por agências federais, impondo a obrigação de que esses órgãos divulguem a existência de registros públicos de informações e de que haja o consentimento por escrito para divulgação de dados de indivíduos por essas entidades, salvo situações excepcionais (VALENTE, 2018).

Sob a óptica institucional, não há um órgão específico que concentre o tratamento dos assuntos e das ocorrências relacionados à proteção da privacidade no país. Seguindo a mesma linha de raciocínio, existem, em âmbito federal, entidades independentes, responsáveis por regular e controlar a aplicação das normas de determinado setor.

Uma agência em especial exerce papel de destaque sobre o tema: ***Federal Trade Commission*** (FTC), criada com o propósito de "proteger os consumidores e a concorrência, evitando práticas comerciais anticompetitivas, enganosas e injustas por meio da aplicação da lei, defesa e educação, sem sobrecarregar indevidamente a atividade comercial legítima"[13]. A comissão dispõe de poder para adotar medidas para garantir o cumprimento de suas regras, bem como poderes de investigação no seu campo de atuação.

Vale destacar que, nos Estados Unidos, há consideráveis práticas de autorregulação, exercidas por meio de iniciativas de entidades privadas (políticas de privacidade, selos e outros mecanismos de certificação), coexistindo um fragmentados regime de corregulação, desempenhado pelas agências setoriais, impondo sanções em função do descumprimento de códigos de conduta, de ética e cláusulas-tipo estabelecidas pelas próprias empresas e homologadas perante o órgão regulador (BNDESa, 2017).

4.3.3 América Latina

No que se refere aos aspectos normativos, diversos países da América Latina já dispõem de legislação específica de proteção de dados, como Chile, Argentina, Uruguai e Colômbia (VALENTE, 2018).

No Chile, a lei foi editada em 1999, estabelecendo limites ao uso dos dados, que, nesse país, deve restringir-se ao propósito informado no ato da coleta, à exceção de registros tornados públicos. Além disso, o texto estabeleceu que o tratamento de dados pessoais pelo Poder Público deve vincular-se ao previsto na lei, impedindo também a divulgação por parte do Governo de informações sobre condenações depois de prescreverem.

Na Argentina, a Lei de Proteção de Dados Pessoais também foi aprovada há alguns anos, em 2000, regulamentando bases de dados públicas e privadas e também pre-

13 https://www.ftc.gov/about-ftc

vendo que seu uso seja adstrito à finalidade para a qual foram obtidos. O tratamento está condicionado ao consentimento do titular, que deve ser livre, expresso e informado, salvo algumas exceções.

O Uruguai, por sua vez, tem desempenhado um papel de destaque na América Latina em relação à proteção de dados pessoais, tendo sido o segundo país da região a obter reconhecimento pela União Europeia de que promove a adequada proteção de dados e o primeiro país não europeu a ratificar a Convenção 108 do Conselho Europeu.

Em termos normativos, foi promulgada a Lei nº 18.331/2008 (*Ley de Protección de Datos Personales y Acción de Habeas Data* – LPDP), que garante ao titular dos dados o direito de controlar o seu uso.

De modo semelhante ao modelo europeu, há um órgão específico, com autonomia técnica, responsável por assegurar o cumprimento desse direito: *Unidad Reguladora y de Control de Datos Personales* (URCDP), possuindo competências de normatização, fiscalização, cooperação, sancionamento, gestão da transferência internacional de dados, consultoria, orientação e assessoramento do Poder Executivo. Em relação às sanções, vale dizer que a URCDP dispõe de poderes para aplicar advertências, multas, suspensão e encerramento de base de dados, promovidas com apoio do Poder Judiciário (BNDESa, 2017).

Quando à estrutura dessa Unidade Reguladora, ela é regida por um Conselho Executivo, assessorado por um Conselho Consultivo multissetorial, composto por representantes do Poder Judiciário, do Ministério Público, da academia, do setor privado, e que possuam reconhecida trajetória na defesa e promoção dos direitos humanos.

Os responsáveis por banco de dados abarcados pela lei devem registrá-lo obrigatoriamente junto à URCDP, que divulga de maneira gratuita a qualquer indivíduo a existência de bancos de dados pessoais, suas finalidades e a identidade dos seus responsáveis.

Há, também nesse caso, mecanismos de corregulação, como a possibilidade de que códigos de conduta formulados por associações e entidades representativas de responsáveis por bancos de dados de titularidade privada sejam registrados junto à URCDP, desde que considerados adequados à legislação (BNDESa, 2017).

4.4 A regulamentação da privacidade no Brasil

Até meados do ano passado, o Brasil figurava como um dos poucos países das maiores economias do mundo que não contava com uma lei geral de proteção de dados, demonstrando o atraso significante em relação a outros países, que vinham regulando o tema há quase 20 anos, como é o caso do Chile.

Ao contrário disso, o Brasil contava com normas esparsas, resumidamente descritas na Tabela 2 a seguir:

Tabela 2: Principais normativos atinentes à proteção da privacidade e dos dados pessoais até 2018

Constituição Federal de 1988	
Garantias ao cidadão	• Art. 5º, X: Direito à inviolabilidade da intimidade e da vida privada; • Art. 5º, LXXII: Habeas Data; • Art. 5º, XII: Direito ao sigilo de comunicações.
Código de Defesa do Consumidor (Lei nº 8.078/1990)	
Regime de responsabilidade civil	• Em relações de consumo aplica-se o regime de responsabilidade objetiva ao fornecedor de serviços;
Direitos do consumidor	• Art. 4º, III: Regime da boa-fé objetiva; • Art. 6º, III: Dever de informação; • Art. 42, § 2°: Notificação por escrito em caso de criação de bancos de dados; • Art. 43, § 3°: Direito de acesso e retificação a informações armazenadas em bancos de dados; • Art. 43, § 1°: Limite de armazenamento de “informações negativas” por até 5 (cinco) anos em base de dados.
Lei Geral de Telecomunicações (Lei nº 9.472/1997)	
Direitos do usuário	• Art. 3º, V: Direito à inviolabilidade e ao segredo de suas comunicações, salvo restrições legais; • Art. 3º, IX: Compartilhamento de dados cadastrais por operadoras de telefonia pode ocorrer mediante decisão judicial fundamentada; • Art. 72, § 2°: Informações agregadas, que não permitam a identificação do usuário, podem ser divulgadas por expressa autorização legal.
Lei do Habeas Data (Lei 9.507/1997)	
Direitos do usuário	• Art. 2º: direito de acesso a informações relativas à pessoa do requerente, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; Art. 3º e seguintes: Ação de Habeas Data.
Código Civil (Lei nº 10.406/2002)	
Proteção aos direitos da personalidade	• Arts. 11 a 21. Rol ilustrativo: proteção ao direito à integridade psicofísica, ao nome e ao pseudônimo, à imagem e à inviolabilidade da vida privada à pessoa natural.

Lei do Cadastro Positivo (Lei 12.414/2011)	
Direitos do consumidor	• Art. 3º, § 3º: Proibição de anotação de informações excessivas ou sensíveis; • Art. 4º: Necessidade de autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada; • Art. 5º e 6º: Dever de informação e transparência com o cadastrado; • Art. 7º: Restrição a utilização das informações constantes dos bancos de dados positivos, as quais somente pode servir para análise de risco de crédito ou para subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.
Lei de Acesso a Informação (Lei 12.527/2011)	
Direitos do indivíduo referenciado	• Art. 31: Dever de tratar informações pessoais de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. • Art. 31, § 1º, I: restrição de acesso pelo prazo máximo de 100 anos. • Art. 31, § 2º: Responsabilização pelo uso indevido de informações pessoais.
Marco Civil da Internet (Lei nº 12.965/2014)	
Direitos do usuário	• Art. 3º: Proteção da privacidade e dos dados pessoais, dentre outros, como princípios do uso da internet no Brasil; • Art. 7º, I e II: Garantia à inviolabilidade da intimidade e da vida privada, do sigilo do fluxo de comunicações pela internet (salvo por ordem judicial).
Proteção de dados pessoais	• Art. 7º, VIII a X: Estabelece princípios na proteção de dados pessoais. » O fornecimento de dados pessoais e registros de conexão e de acesso a aplicações de internet a terceiros deverá ser precedido da obtenção de consentimento; Obrigação de prestar informações claras; » A coleta deverá observar a obtenção de consentimento expresso, livre, informado e destacado; » Obrigação de exclusão de dados pessoais, caso requerido pelo titular de dados.
Obrigação de retenção de dados de conexão e de acesso a aplicações	• Art. 10 a 17: Obrigações na guarda de registros e dados pessoais. » A guarda e disponibilização de registro de conexão e de acesso a aplicações deve atender à preservação da intimidade, vida privada, honra e imagem; » Armazenamento de registros de acesso por aplicações de internet pelo período de 6 (seis) meses; » Armazenamento de registro de provisão de conexão de conexão à internet pelo período de 1 (um) ano; » Para acesso aos dados de registro, o interessado deverá obter autorização judicial prévia; • Dados cadastrais que informem qualificação pessoal, filiação e endereço podem ser acessados por autoridade administrativa com competência legal para a requisição.

Regulamento do Marco Civil da Internet (Decreto nº 8.771/2016)	
Proteção de dados pessoais	• Art. 14: Definição de "dados pessoais" e "tratamento de dados pessoais"; • Art. 13: Obrigação de exclusão de dados tão logo atingida a finalidade ou se encerrado o prazo determinado por obrigação legal
Segurança	• Art. 13: Diretrizes de segurança a provedores de conexão e aplicações: (i) mecanismos para autenticação de acesso aos registros; (ii) criação de inventário de histórico de acesso; (iii) sugestão de adoção de criptografia ou meio equivalente para segurança dos dados.

Fonte: BNDES b, 2017, p. 47.

Embora abarcassem importantes preceitos, essa fragmentação de normativos relacionados à proteção dos dados pessoais no país, com aplicações específicas a determinados contextos, gerava um ambiente de insegurança jurídica.

Essa sensação de insegurança, no contexto da Internet das Coisas, agravava-se, não apenas diante dos novos modelos de negócio e das soluções inovadoras, cuja compreensão sequer era alcançada por boa parte das pessoas que não mantêm relação direta com o estudo do tema, mas também pelos riscos de que práticas abusivas fossem cometidas em decorrência de lacunas interpretativas nas diversas normas que abordavam o assunto, tendo em vista a perspectiva da ocorrência de inúmeras situações ainda não experimentadas pelas pessoas nessa nova realidade altamente conectada.

Isso incluía o Brasil no rol dos países "não seguros" em relação à proteção de dados pessoais, impedido, inclusive, a manutenção de plenas relações com os integrantes da União Europeia, bem como outros países que, para determinadas atividades, exigiam igual ou maior proteção do que a oferecida em seu ordenamento pátrio (COTS; OLIVEIRA, 2018).

De modo a contornar esse cenário, oferecendo às comunidades global e nacional as bases legais da proteção de dados, por meio de um conjunto de normas específicas sobre o tema, consolidadas em um normativo único, foi sancionada, em 14/08/2018, a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados no Brasil (LGPD), posteriormente alterada pela Medida Provisória nº 869/2018. A norma passará a vigorar integralmente em dois anos da sua data de publicação, em 2020, de modo que ainda sem encontra no período de vacatio legis.

A nova lei é oriunda de um projeto de lei que tramitava há anos na Câmara dos Deputados (PL 4060/2012) e tem forte inspiração no GDPR da União Europeia, mencionado em tópico anterior deste artigo, como reconhecido pelo próprio Senado Federal[14].

14 https://www12.senado.leg.br/noticias/materias/2018/07/03/regras-para-protecao-de-dados-pessoais-saoaprovadas-e-vao-a-plenario

A lei foi sancionada tendo como objetivo "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", definindo como dado pessoal a "informação relacionada à pessoa natural identificada ou identificável". Ou seja, segundo a norma, qualquer informação que identifique ou possibilite a identificação de um indivíduo encontra-se amparada pela lei.

O regramento introduziu importantes conceitos e regras, abrangendo diversos aspectos relevantes relacionados à coleta e ao tratamento de dados no país, exemplificados na Tabela 3:

Tabela 3: O tratamento de dados pessoais nos ditames da Lei nº 13.709/2018

Aplicação territorial	• Aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
Princípios a serem respeitados nas atividades de tratamento de dados pessoais	• Finalidade: os dados devem ser tratados para os fins legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com seu propósito original; • Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; • Necessidade: limitação do tratamento ao mínimo necessário, só devendo ser coletados os dados pertinentes, proporcionais e não excessivos em relação às finalidades pretendidas. • Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma, a integralidade e a duração do tratamento de seus dados; • Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; • Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; • Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; – Segurança: dever de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; • Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; • Responsabilização e prestação de contas: demonstração, pelo agente de tratamento de dados, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas.

Consentimento para o tratamento dos dados pessoais	• O tratamento de dados pessoais depende do consentimento expresso por seu titular, para um período determinado. Ele deve ser explícito e fornecido para um fim específico. O consentimento pode ser revogado a qualquer momento pelo titular. • A comunicação ou o compartilhamento de dados pessoais com outros controladores necessita de consentimento específico para esse fim.
Principais direitos dos titulares dos dados	• Direito de confirmação do tratamento de dados, de acesso e correção de dados incompletos, inexatos ou desatualizados; • Direito à anonimização dos seus dados, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei; • Direito à portabilidade dos dados a outro fornecedor de serviço ou produto (contratos de seguro de saúde ou abertura de contas correntes, por exemplo); • Direito à eliminação dos dados pessoais tratados com o consentimento do titular; • Direito à informação das entidades públicas e privadas com as quais houve uso compartilhado de dados; • Direito à revogação do consentimento.
Transferência internacional de dados	• A transferência internacional de dados pessoais somente será permitida para países que proporcionem grau de proteção de dados pessoais adequado ao previsto na lei, ou quando houver comprovadas garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na norma.
Responsabilidade e ressarcimento de danos	• O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo; • Responsabilidade solidária dos agentes de tratamento de dados.
Sanções em caso de descumprimento da lei	• Advertência, com prazo para adoção de medidas corretivas; • Multa simples, de até 2% do faturamento da empresa, grupo ou conglomerado no Brasil, limitada a R$ 50 milhões por infração; • Multa diária, observado o limite total de R$ 50 milhões; • Publicização da infração após devidamente apurada e confirmada; • Bloqueio dos dados pessoais associados à infração até sua regularização; • Eliminação dos dados pessoais a que se refere a infração.

Fonte: Autoria própria

Um ponto que merece destaque do normativo refere-se às regras estabelecidas para os órgãos e as entidades governamentais. De acordo com o art. 23 da lei, o tratamento de dados pessoais pelas pessoas jurídicas de direito público deve ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de cumprir as atribuições legais do serviço público.

Nesse caso, devem ser obrigatoriamente informadas as hipóteses em que essas instituições, no exercício de suas competências, realizam o tratamento de dados pessoais, de a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a

execução dessas atividades, em veículos de fácil acesso, de forma clara e atualizada, preferencialmente em seus sítios eletrônicos. Deve também ser indicado um encarregado quando da realização de operações de tratamento de dados pessoais.

Além disso, como disposto nos art. 26 e 27, o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no normativo, sendo necessário o consentimento do titular.

Tendo em vista que, como anteriormente analisado, o mau uso de informações pessoais pode coibir a liberdade de expressão dos cidadãos e comprometer, inclusive, a própria democracia, os dispositivos da lei foram relevantes, no sentido de buscar limitar os contextos informacionais no âmbito da Administração Pública e prevenir práticas abusivas e monitoramento excessivo por parte do Governo.

Vale dizer que as regras se aplicam aos órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; bem como às autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

O normativo também estabelece seção específica para a proteção de dados sensíveis (referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural) e de crianças e de adolescentes;

Há ainda a previsão de mecanismos de autorregulação, estando expressa, no art. 50, a possibilidade de os responsáveis pelo tratamento de dados, individualmente ou por meio de associações, formulem regras de boas práticas e de governança. Caso sejam estabelecidas, essas regras deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Uma das principais mudanças introduzidas pela lei no tocante ao sistema institucional de proteção de dados do país, foi a criação de um órgão específico, responsável por zelar, implementar e fiscalizar o seu cumprimento, denominado Autoridade Nacional de Proteção de Dados (ANPD).

Embora sua criação já estivesse estabelecida no texto final aprovado pelo Senado Federal, ela foi objeto de veto presidencial, em função de alegada inconstitucionalidade dos dispositivos, tendo sido efetivada pouco depois por meio da Medida Provisória nº 869, de 27/12/2018, que alterou, portanto, a Lei de Proteção de Dados.

Assim, consoante atualmente disposto na norma geral, o órgão central será composto, entre outros por (i) um Conselho Diretor, formado por seis membros, indicados pelo Presidente da República para mandatos de quatro anos, que ocuparão cargos em comissão do GrupoDireção e Assessoramento Superior - DAS de nível 5; e pelo (ii) Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, formado por 23 representantes não remunerados, sendo: um do Poder Executivo Federal; um do Senado Federal; um do Câmara dos Deputados; um do Conselho Nacional de Justiça; um do Conselho Nacional do Ministério Público; um do Comitê Gestor da Internet no Brasil; quatro de entidades da sociedade civil; quatro de instituições científicas, tecnológicas e de inovação; e quatro de entidades representativas do setor empresarial.

Foram conferidas amplas e importantes atribuições à ANPD, exercidas por meio do Conselho Diretor, contando, inclusive, com poderes para editar normas; deliberar, na esfera administrativa, sobre a interpretação da lei, suas competências e os casos omissos; requisitar informações a qualquer momento a qualquer agente que trate dados pessoais, públicos ou privados; tratar reclamações dos usuários; fiscalizar e aplicar sanções; estimular a adoção de padrões para serviços e produtos; promover ações de cooperação com autoridades de outros países; articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais, entre outras atribuições.

O Conselho Nacional, por sua vez, tem características de um órgão de assessoramento, com competência para propor diretrizes estratégicas, ações, elaborar relatórios anuais e estudos, realizar debates e disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral.

Embora fosse há muito desejada e discutida, a criação do Conselho Diretor responsável pela guarda e proteção dos dados pessoais de todos os indivíduos em território nacional, no formato aprovado pela Medida Provisória nº 809/2018, editada a quatro dias do final do exercício, deixou lacunas que podem trazer impactos imensos à política nacional de proteção de dados, comprometendo, inclusive, a efetividade de todo o normativo.

Primeiramente, o art. 55-A, que efetivamente estabelece a criação do órgão, deixa expresso que ele é integrante da Presidência da República, sem status de autarquia ou agência. Ou seja, a Autoridade Nacional e Proteção e Dados está diretamente vinculada ao Chefe do Poder Executivo.

Vale dizer que o texto originalmente saído do Congresso Nacional, requeria explicitamente a criação de uma "entidade integrante da administração pública federal indireta, submetida a regime autárquico especial". Dessa forma, no formato aprovado, a ANPD perde sua autonomia institucional, requisito absolutamente essencial para o tratamento de questões de tamanha relevância e sensibilidade, como a proteção da privacidade dos indivíduos e o controle do uso de dados pessoais.

Sem essa garantia de independência institucional, as autoridades – e, consequentemente, as atividades por elas desempenhadas – tornam-se suscetíveis a influências políticas e econômicas, podendo deixar de exercer suas atribuições de forma imparcial, em prol do melhor interesse público das decisões.

Ademais, o art. 45 do GDPR da União Europeia estabelece que a transferência de dados pessoais a outros países depende da existência e do efetivo funcionamento de uma ou mais autoridades de controle independentes. Em outras palavras, nos moldes aprovados, ainda que a lei tenha trazido inúmeros avanços e importantes regras em seus dispositivos, o Brasil permanece fora do rol de países aptos a acessar dados de milhares de cidadãos europeus, mantendo-se a par dos diversos fluxos de dados internacionais que poderiam surgir de acordos cooperativos, bem como das oportunidades de negócio deles advindas.

Nesse mesmo sentido, é notório que o poder decisório concentra-se no Conselho Diretor, sendo o Conselho Nacional um órgão meramente consultivo, formado por cidadãos que não serão remunerados pelo desenvolvimento dos trabalhos.

Nesse contexto, outro problema que se vislumbra reside no fato de todos seus membros, sem exceção, serem indicados pelo Presidente da República. Embora o texto não impute expressamente ao Presidente a responsabilidade por essa indicação, sendo omisso a respeito de como se daria esse processo, é o que se depreende da leitura dos dispositivos a seguir:

> "Art. 55-D. O Conselho Diretor da ANPD será composto por cinco diretores, incluído o Diretor-Presidente.
>
> §1º **Os membros do Conselho Diretor da ANPD serão nomeados pelo Presidente da República e ocuparão cargo em comissão** do GrupoDireção e Assessoramento Superior - DAS de nível 5.
>
> §2º Os membros do Conselho Diretor **serão escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos** para os quais serão nomeados.
>
> §3º O mandato dos membros do Conselho Diretor será de quatro anos." (Lei nº 13.709/2018, grifo nosso)

Nesse mesmo sentido, todos os cargos em comissão e funções de confiança da Autoridade Nacional serão indicados pelo Conselho Diretor, ou seja, os indicados pelo Presidente da República, indicarão todos os demais integrantes do órgão.

No que concerne à autonomia orçamentária, requisito mencionado na literatura como fundamental à imparcialidade e equidade na execução das atividades e tomada de decisões, há a previsão expressa na lei de que o órgão será criado sem aumento de despesas da União, significando que os cargos serão remanejados de outras estruturas do Poder Executivo, sendo todos os ocupantes indicados pelo Conselho Diretor, como mencionado (art. 55-H e 55-I).

Com isso, a instituição não dispõe de orçamento próprio para decidir, a seu critério e de modo imparcial, as ações prioritárias, as normas, as sanções e demais relevantes poderes a ela conferidos pela lei. Há que se destacar que, embora a efetiva criação de uma autoridade central de supervisão do uso de dados pessoais possa resultar em novos gastos ao Governo, é importante que se tenha a clara compreensão de que ela é absolutamente necessária para a efetividade das leis, o desenvolvimento do país e a proteção dos cidadãos. Sobre isso, Danilo Doneda (2018), professor no IDP e UERJ, advogado e consultor do CGI.br, expõe que:

> "Em primeiro lugar, **a Autoridade é elemento indispensável para que os direitos e garantias dos cidadãos sobre seus dados sejam efetivamente implementados e monitorados**. (...) o tratamento de dados pessoais é uma atividade complexa e que muitas vezes acontece de forma opaca, sendo realizado por entidades e corporações cujas práticas não são suficientemente transparentes – e que podem ser abusivas. A existência de uma Autoridade que **atue de forma coordenada para prevenir e reprimir abusos, fiscalizando e tutelando tratamentos de dados** de inteiras coletividades **é fundamental para diminuir a distância abissal entre o cidadão e os entes que tratam seus dados** (...).
>
> (...) **uma Autoridade pode manter padrões persistentes de aplicação da lei, diferentemente de tribunais**, que são em geral chamados a decidir sobre situações particulares. Esta consistência, aliás, também é importante para **impedir que uma determinada empresa que não cumpra a LGPD possua vantagens competitivas** em relação às demais, com prejuízo para os cidadãos. Ainda, a Autoridade possui um arsenal mais rico e específico de medidas regulatórias à sua disposição (...) Isto, somado ao fato de que a centralização da matéria em uma **Autoridade evita o risco certo de fragmentação da interpretação da lei** entre tribunais e mesmo outros órgãos administrativos com competências eventualmente concorrentes, garante a uniformidade dos direitos do cidadão e a segurança jurídica na aplicação da LGPD.
>
> (...) Ao mesmo tempo, os efeitos cada vez mais intensos do tratamento de dados pessoais na vida dos cidadãos implicam na **necessidade**

> **de proporcionar garantia rápida a direitos** cujos contornos podem ser bastante fluídos." (grifo nosso)

As fragilidades destacadas abrem espaço a um incontável número de possíveis prejuízos à política recentemente implementada por meio da Lei Geral de Proteção de Dados, especialmente considerando-se o elevado poder conferido pela norma ao Conselho Diretor, por meio de competências normativas e fiscalizatórias.

Considerando-se a alta ramificação em termos de setores econômicos regulados, aspectos monitoráveis da vida dos indivíduos, quantidade de informações coletáveis, pulverização dos agentes, complexidade dos temas e outros aspectos tratados anteriormente acerca da Internet das Coisas, a vulnerabilidade do órgão central a interferências indesejadas e a concentração de poderes exclusivamente no Presidente da República afeta diretamente a efetividade da norma publicada.

D. Doneda (2018) destaca a importância desses requisitos, em análise prévia à efetiva criação da ANPD:

> "Para que desempenhe com eficácia estas funções, **alguns atributos e características mínimas da Autoridade deverão ser observadas, sob pena de que a LGPD, aprovada com apoio transversal da Sociedade, permaneça apenas 'no papel**'.
>
> Destas características, a **independência e autonomia são essenciais.** A Autoridade possui a função maior de **garantir os direitos dos cidadãos sobre seus dados**. Como os dados pessoais são hoje tratados pelos setores público e privado, esta função de garantia **somente pode ser exercida de forma eficaz caso seja garantida a independência da Autoridade**. A Autoridade possui igualmente **relevantíssima função regulatória** para os diversos implicados no tratamento de dados – posto que a clareza e transparência que derivam da definição dos direitos e garantias dos cidadãos proporciona um ambiente regulatório com maior segurança jurídica para quem trate dados pessoais.
>
> Para que se caracterize esta necessária independência, as atividades fiscalizatória, sancionatória e decisional da Autoridade não **poderão estar de forma alguma subordinadas hierarquicamente a outros órgãos**. (...)
>
> **Uma Autoridade independente, com autonomia técnica e dotada dos meios necessários para realizar suas funções é, portanto, condição orgânica para que as garantias presentes na LGPD sejam eficazes**. E, ainda, **é uma peça indispensável para que o Brasil**

> **obtenha as vantagens econômicas e políticas derivadas da LGPD: por exemplo, a obtenção da adequação europeia** (garantindo livre fluxo de dados entre o Brasil e os países do bloco) **depende inexoravelmente do estabelecimento de uma Autoridade independente; o ingresso do Brasil na OCDE pode ser facilitado, entre outros**. De forma geral, o comércio internacional vem apresentando requisitos mais concretos quanto à proteção de dados, sendo um destes a **existência de uma Autoridade independente como condição para que empresas ou órgãos brasileiros possam participar livremente de fluxos internacionais de dados, tão caros à nova economia da informação**. Neste sentido, destaque-se recente acordo entre **União Europeia e Japão que consolidou a maior área de livre fluxo de dados do mundo, tornado possível principalmente com o estabelecimento de uma Autoridade independente para a proteção de dados pelo Japão**. Um acordo como este facilita o acesso de empresas japonesas a um mercado de **mais de quinhentos milhões de consumidores**.
>
> (...) **a consideração integral e a longo prazo das consequências da adoção de um determinados modelo institucional parece, mais do que nunca, o ponto mais sensíve**l para que se determinem os **reais efeitos modernizadores que a lei terá** para a Sociedade e o país" (grifo nosso).

Por fim, a publicação da Lei 13.709/2018 pode ser considerada um marco na proteção dos dados pessoais e na vida privada dos cidadãos, sendo de grande relevância dentro do contexto atual e das perspectivas de um futuro bastante desafiador, no que diz respeito a esse tema.

No entanto, para que uma norma efetivamente atenda e cumpra sua missão de servir aos indivíduos e à coletividade, não basta que ela seja editada. É necessário que sua aplicação seja tratada como prioridade pelo Governo, no sentido de conceder aos envolvidos todos os instrumentos possíveis para que ela seja adequadamente cumprida, e que o seu processo de implementação seja feito com o propósito de resguardar os direitos fundamentais dos cidadãos e o interesse público.

5. Conclusão

No contexto da Internet das Coisas, as perspectivas apontam no sentido de que a realidade já hoje experimentada, em que o cotidiano das pessoas é cercado de dispositivos conectados à Internet, com capacidade de coletar e processar um incontável número de dados, será, em muito, intensificada nos próximos anos. Praticamente todos

os aspectos do dia-a-dia das pessoas passarão a ser, de alguma forma, monitorados ou monitoráveis.

Embora seja inegável que a evolução tecnológica vivenciada nas últimas décadas, em especial a partir do advento da Internet, trouxe inúmeros benefícios à sociedade e à vida das pessoas em geral, há que considerar que a coleta massiva de dados pessoais traz também diferentes consequências e riscos relacionados à privacidade dos indivíduos.

Informações pessoais relacionadas a práticas esportivas, condições físicas, saúde, hábitos alimentares e sociais, preferências político-religiosas, interesses pessoais, qualidade do sono, entre outras, vindas de diferentes fontes e ambientes de coleta, além de efetivamente exporem as pessoas a um constante monitoramento, permitirão infinitos cruzamentos de dados que trarão novas informações acerca de cada um.

Juntamente à exposição da vida privada das pessoas, esse conjunto de dispositivos capazes de observar e "sentir" o ambiente em que estão dão origem a outros riscos, associados à ampliação da vigilância governamental; ao compartilhamento e à comercialização dos dados entre pessoas e empresas de forma não-consentida pelo titular; e à pouca transparência do caminho perseguido pela informação coletada.

Nesse sentido, tem crescido, nas últimas décadas, o debate mundial acerca do direito à privacidade e à proteção dos dados pessoais, no intuito de antecipar consequências danosas aos cidadãos, bem como evitar ou mitigar alguns riscos que deverão se intensificar nos anos subsequentes.

Alguns países já vêm desenvolvendo normas e legislações atinentes ao tema há anos, possuindo legislações especificamente destinadas à proteção de dados pessoais de seus cidadãos há mais de duas décadas. É o caso do Chile, União Europeia e Argentina, por exemplo. Outros, contam com legislações esparsas, como é tipicamente o caso dos Estados Unidos.

O Brasil, até meados do ano passado, figurava como um dos poucos países das maiores economias do mundo que não contava com uma lei geral de proteção de dados. O tema era tratado por meio de leis esparsas, normalmente vinculadas a um setor específico de atividade.

Essa fragmentação no tratamento do tema criava um ambiente de insegurança jurídica que, no contexto da Internet das Coisas, agravava-se diante dos novos modelos de negócio e das soluções inovadoras, bem como dos riscos de que práticas abusivas fossem cometidas em decorrência de lacunas interpretativas nas diversas normas que abordavam o assunto. Isso incluía o Brasil no rol dos países "não seguros" em relação

à proteção de dados pessoais, impedido, inclusive, a manutenção de plenas relações com determinados países.

De modo a contornar esse cenário, oferecendo às comunidades global e nacional as bases legais da proteção de dados, foi publicada a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados no Brasil – LGPD, alterada pela Medida Provisória nº 869/2018, que pode ser considerada um marco na proteção dos dados pessoais e na vida privada no país.

Contudo, há graves fragilidades no desenho institucional estabelecido pelos normativos, no que se refere à governança do órgão central criado para zelar pela sua aplicação, que conta com poderes normativos, fiscalizatórios e sancionatórios.

Essas fragilidades, entre outras coisas, criam um ambiente não-seguro em relação a influências político-econômicas na aplicação da nova política de dados, que pode resultar em decisões governamentais baseadas em interesses pessoais, em prejuízo ao melhor interesse público e à proteção da privacidade dos cidadãos.

Vale lembrar que a garantia à proteção dos dados pessoais perpassa não só pelo campo pessoal, sendo direito fundamental estabelecido pela Constituição Federal, mas também pelo coletivo, posto que é essencial para assegurar a participação imparcial dos cidadãos na vida política, bem como a liberdade de expressão. Nesse sentido, o direito à privacidade não visa apenas à proteção do indivíduo, mas também à manutenção de um verdadeiro estado democrático de direito.

Tendo em vista o pouco tempo de publicação da norma, há que se atentar também para o seu processo de estruturação e aplicação, buscando assegurar que seja tratado como prioridade pelo Governo, no sentido de conceder aos envolvidos todos os instrumentos possíveis para que seu efetivo cumprimento com o propósito de resguardar a vida privada, a segurança, a liberdade e o direito à privacidade dos usuários dos serviços.

Referências Bibliográficas

ROSNER, Gilad; KENNEALLY, Erin. Clearly Opaque: Privacy Risks of the Internet of Things. The Internet of Things Privacy Forum. 2018;

ROSNER, Gilad. Privacy and The Internet of Things. 1ª ed. Califórnia, EUA: O'Reilly Media, Inc., 2016;

ASHTON, Kevin. That 'Internet of Things' Thing. 2009. Disponível em: <https://www.rfidjournal.com/articles/view?4986>. Acesso em 24/02/2019;

NSTAC US NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE. Report to the President on the Internet of Things. 2014. Disponível em: <https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Repo rt%2011-2014.pdf>. Acesso em 24/02/2019;

UIT UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. Recomendação ITUT Y.2060. 2012. Disponível em: <http://handle.itu.int/11.1002/1000/11559>. Acesso em 24/02/2019;

BNDESa BANCO NACIONAL DE DESENVOLVIMENTO; MCTIC MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. Internet das Coisas: um plano de ação para o Brasil. Relatório 8B. 2017. Disponível em: < https://www.bndes.gov.br/wps/wcm/connect/site/f9582d36-4355-4638-b931e2e53af5e456/8B-relatorio-final-plano-de-acao-produto-ambienteregulatorio.pdf?MOD=AJPERES&CVID=m7tyLs1>. Acesso em 24/02/2019;

BNDESb BANCO NACIONAL DE DESENVOLVIMENTO; MCTIC MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. Internet das Coisas: um plano de ação para o Brasil. Relatório 3E. 2017. Disponível em: < https://www.bndes.gov.br/wps/wcm/connect/site/e614e9a3-053b-42d4-853a6b4aa406e31f/produto-3-analise-de-oferta-e-demanda-relatorio-horizontal-ambienteregulatorio.pdf?MOD=AJPERES&CVID=lWrmVlj>. Acesso em 24/02/2019;

CURTIN UNIVERSITY. Introduction to the Internet of Things (IoT). EdX Courses. 2019. Disponível em: <https://www.edx.org/course/introduction-to-the-internet-ofthings-iot-1>. Acesso em 14/01/2019;

BRIDGERA LLC; RIOT. A Reference Guide to the Internet of Things. 1ª ed. Carolina do Norte, EUA: Bridgera LLC, 2017. Disponível em: <https://bridgera.com/wpcontent/uploads/2018/10/IoTeBook3.pdf >. Acesso em 24/02/2019;

ZANINI, Leonardo Estevam de Assis. O Surgimento e o Desenvolvimento do Right of Privacy nos Estados Unidos. Revista Brasileira de Direito Civil. São Paulo, v.3, p. 827, 2015. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/107/103>. Acessado em: 26/02/2019;

GAVISON, R. Privacy and the Limits of the Law. Yale Law Journal, v. 89, n. 3, p. 421-471. 1980. Disponível em: <https://digitalcommons.law.yale.edu/ylj/vol89/iss3/1/>. Acessado em 24/02/2019;

CISCO. Cisco Visual Networking Index: Forecast and Trends, 2017–2022. 2019. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visualnetworking-index-vni/white-paper-c11-741490.pdf>. Acessado em 07/03/2019;

PATTERSON, Heather. Contextual Expectations of Privacy in Self-Generated Health Information Flows. 2013. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2242144>. Acessado em 24/02/2019;

ACKERMAN, Linda. Mobile Health and Fitness Applications and Information Privacy. 2013. Disponível em: <http://www.privacyrights.org/sites/default/files/mobile-medical-apps-privacyconsumer-report.pdf>. Acessado em 24/02/2019;

SOLTANI, Ashkan. What's the security shelf-life of IoT? 2015. Disponível em: <https://www.ftc.gov/news-events/blogs/techftc/2015/02/whats-security-shelf-lifeiot>. Acessado em 24/02/2019;

ACKERMAN, S.; THIELMAN, S. US intelligence chief: we might use the internet of things to spy on you. The Guardian. 2016. Disponível em: <https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smarthome-devices-government-surveillance-james-clapper>. Acessado em 24/02/2019;

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Poder Executivo, Brasília, DF, 15/08/2018, seção 1, p. 59;

BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Diário Oficial da União, Poder Executivo, Brasília, DF, 28/12/2018, seção 1, p. 8;

UNIÃO EUROPEIA. CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. 2000. Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex:12016P/TXT>. Acessado em 26/02/2019;

UNIÃO EUROPEIA. Diretiva 95/46/CE. 1995. Disponível em: <https://eurlex.europa.eu/legal-content/PT/ALL/?uri=celex%3A31995L0046>. Acessado em: 26/02/2019;

VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. 2018. EBC. Disponível em: <http://agenciabrasil.ebc.com.br/politica/noticia/201805/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises>. Acessado em: 26/02/2019;

COTS, Márcio; OLIVEIRA, Ricardo. 10 Impactos da Lei Geral da Proteção de Dados. 2018. Disponível em: <https://www.itforum365.com.br/mercado/10-impactosda-lei-geral-da-protecao-de-dados/>. Acessado em: 26/02/2019;

DODEDA, Danilo. O que está em jogo com a nova Autoridade Nacional de Proteção de Dados. 2018. Disponível em: <https://cartoriosdeprotestorj.com.br/o-que-esta-emjogo-com-a-nova-autoridade-nacional-de-protecao-de-dados/>. Acessado em: 26/02/2019

Instituto Serzedello Corrêa

Missão

Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo

Visão

Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável

TRIBUNAL DE CONTAS DA UNIÃO

tcu.gov.br/isc