A INTERNET DAS COISAS E O SISTEMA JURÍDICO BRASILEIRO: NOÇÕES PRELIMINARES DE RESPONSABILIDADE CIVIL IMPOSTA AOS FORNECEDORES DE PRODUTOS E SERVIÇOS

Paulo Roberto Binicheski

Doutorando em Justiça Administrativa pela Universidade Federal Fluminense (UFF); mestre em Ciências Jurídicas pela Universidade de Lisboa; promotor de Justiça de Defesa do Consumidor (MPDFT)

Plínio Lacerda Martins

Doutor em Direito e Sociologia pela Universidade Federal Fluminense (UFF); professor do Programa de Pós-Graduação em Direitos Instituições e Negócios da UFF.

RESUMO

A internet das coisas (*IDC* ou *IoT*, na expressão utilizada em língua inglesa) é um conceito que representa a rede de dispositivos inteligentes (ou "coisas") conectados à Internet e uns aos outros, com a capacidade de coletar, compartilhar e tratar os dados sobre todos os aspectos de nossos negócios e de nossas vidas, queiramos ou não.

Com a ampla disseminação da utilização da Internet, recrudesceram os problemas jurídicos com o uso das funcionalidades da rede e na *IDC* há questões complexas na coleta, tratamento e compartilhamento dos dados dos consumidores, da invasão por hackers de dispositivos, com capacidade de gerar danos materiais e danos à integridade física das pessoas, de dispositivos defeituosos e com vícios de utilidade.

Como e a quem imputar a responsabilidade civil pelos danos causados aos consumidores é a proposta do presente ensaio, mediante a abordagem de casos reais em curso nos Estados Unidos e a sua análise com o regramento jurídico do Brasil.

Palavras-chave: Direito da Sociedade da Informação. Internet das coisas. Casos dos Estados Unidos da América. Direito brasileiro. Código de Defesa do Consumidor.

SUMMARY

The Internet of Things (IoT) is a concept that represents the network of intelligent devices (or "things") connected to each other and to the Internet, with the ability to collect, share and treat data on all aspects - personal and professional - of our lives, regardless of our will or consent.

With the spread of the Internet, the legal problems arising from the use of the various functionalities available on the network have been exacerbated. In the IOT there are complex

issues regarding the collection, processing and sharing of consumer data, as well as the issue of hacker invasion. These factors have the ability to generate defective devices or utility vices, as well as material damage and damage to people's physical integrity.
The purpose of this essay is to address how and who to assign civil liability for damages to consumers by submitting actual cases of the United States and their analysis in accordance with the regulation of Brazil
Keywords: Right of the Information Society. Internet of things. Cases of USA. Brazilian law. Consumer Protection Code.

Introdução

Os avançados meios informáticos propiciam em um mundo cada vez mais globalizado a alavancagem dos negócios no formato eletrônico (*e-business*), ou melhor aduzindo, o comércio tradicional está paulatinamente superado pelo Comércio Eletrônico (*e-commerce*) e há o surgimento de uma variedade de dispositivos inteligentes utilizados no cotidiano das pessoas, permitindo e necessitando de conexão em rede de Internet para suas as plenas funcionalidades. Por um lado, há o incremento de usos de e por outro ocorrem fatos jurídicos decorrentes do uso das coisas, e na linha do adotado pelo nosso Código de Defesa do Consumidor, surgem questões em que se discute a responsabilidade civil pelo fato do produto ou do serviço, considerados como acidente de consumo ou pelo mau funcionamento ou não funcionamento das coisas, o que se pode denominar de vícios de qualidade ou de quantidade.

O Direito do Consumidor, com regramento no Código de Defesa do Consumidor ainda parece ser um novidade e resolver essas intrincadas relações jurídicas advindas da era da Sociedade da Informação até a Internet das Coisas implica, necessariamente, de reflexão serena para evitar interpretações causadoras de insegurança jurídica, de desestímulo a utilização das facilidades obtidas para o setor produtivo, com diminuição de custos e alcance global, tornando os negócios atrativos aos fornecedores, sem descurar da necessária proteção ao consumidor. Para além do Direito do Consumidor, ainda há outras leis esparsas que regulam diversas situações da era da Sociedade da Informação e da Internet das Coisas.

A fase vivenciada era da Sociedade da Informação constata de forma serena ser a informação altamente valiosa para as interações sociais e para os negócios. Nas interações sociais, as pessoas quase que automaticamente adicionam pessoas de seus interesses nas redes sociais e no âmbito dos negócios a publicidade é direcionada para os interesses demonstrados nessas redes sociais. Essas não tão novas formas de interação decorrem diretamente da Internet e de suas notáveis funcionalidades, a face mais visível da era da Sociedade da Informação.

Para este ensaio, há um breve esboço de noções da era da Sociedade da Informação e do vínculo com a Internet e desaguando na era da Internet das Coisas, um fenômeno decorrente da própria disseminação das funcionalidades de objetos conectados em rede. Após, uma abordagem de questões emblemáticas a ser resolvidas pelo advento da Internet, estudo de casos recolhidos em sede de Direito Comparado e seguindo com propostas de solução tomando a base do sistema jurídico brasileiro, notadamente pelas normas existentes, em vigência e regras legais que em breve devem ser aplicadas, por força de lei ainda no período de *vacatio legis*.

Assim sendo, este breve ensaio parte de algumas noções gerais da Sociedade da Informação, narrando algumas nuances da era da Internet das Coisas com exame de casos concretos verificados nos Estados Unidos da América, país com regime jurídico distinto do Brasil e passa a investigar como resolver questões com base em nosso sistema jurídico. Desde já a advertência de que as propostas a ser esboçadas ao longo do ensaio não pretendem esgotar as facetas dos problemas jurígenos que ocorrem com as notáveis funcionalidades da Internet das Coisas. Longe disso, é apenas um início de uma longa discussão.

1 Noções gerais da sociedade da informação

Na virada do milênio, o uso do conceito de Sociedade da Informação já se tornara generalizado e não era apenas um termo cotidiano no vocabulário das

ciências sociais, mas de uso preferido por aqueles envolvidos no planejamento político, no marketing político e no mundo dos negócios (KARVALIC, 2010, p. 13). E deve ser lembrado, o termo Sociedade da Informação penetrou triunfalmente na linguagem da mídia escrita e eletrônica e é exatamente por causa dessa repentina popularidade que o conteúdo da expressão foi "diluído" e na atualidade seu uso está carregado de contradições e de imprecisão terminológica (*ibem, ibidem*).

Com a popularidade alcançada para a era da Sociedade da Informação, os mais variados conceitos foram propostos e alguns até exagerados, e o fato é que existem inúmeras teorias para explicá-la, com a abordagem de diferentes áreas da ciência construída sobre tradições divergentes. Assim, em vez de uma sistematização baseada em "códigos compartilhados ou comuns" há uma batalha constante entre conceitos individuais e conceitos que pretendem ser originais da Sociedade da Informação (*idem,* p. 14)

Na língua portuguesa encontramos, por exemplo, a digressão anotada por alguns professores das ciências jurídicas. Assim, Oliveira Ascensão toma o termo Sociedade da Informação como um slogan, denominando de categoria indefinida, e restringe o alcance apenas ao fenômeno decorrente das próprias transformações ocorridas na sociedade pela difusão da tecnologia, o chamado paradigma digital, formado pelo advento da Internet (ASCENSÃO, 2001, p. 70). Na mesma linha, Dario Moura Vicente aduz a ser a era da Sociedade da Informação como um fenômeno de contornos ainda não inteiramente definidos (VICENTE , 2005, p. 14) ou como afirma Catrin Pekari, o termo em si ainda não foi definido de forma satisfatória e nem suas implicações são totalmente claras (PEKARI, 2005, p. 58).

O termo Sociedade da Informação não nasceu na Europa, muito embora a literatura brasileira mais recente assim afirme (MARTINS, 2014, p. 4), e isso decorre das enormes discussões no seio da comunidade europeia visando a implementação do acesso aos bens e serviços decorrentes das novas tecnologias. No entanto, a origem do

termo Sociedade da Informação está no Oriente, particularmente no Japão onde teriam ocorrido os primeiros marcos teóricos com a abordagem do tema em caráter científico.

Efetivamente, a literatura aponta as possíveis origens do termo Sociedade da informação àquele país insular, com a afirmação do possível marco inicial decorrente de uma conversa ocorrida em 1961 entre o historiador e antropólogo Tadao Umesao e o arquiteto Kisho Kurokawa. (DUFF, 2000) Desse modo, Duff lembra os escritos de Youichi Ito, no qual esse autor afirma que a difusão do termo Sociedade da Informação adveio do ensaio intitulado "Joho sangyo ron" de Tadao Umesao publicado em 1963, ao referir sobre a indústria da informação.[194]

O primeiro escrito com a utilização do termo teria sido atribuído ao editor Michiko Igarashi, em *"Sociology in Infomation Societies"*, fatos que originaram uma discussão sobre quem efetivamente teria cunhado a expressão Sociedade da Informação pela primeira vez.[195] Há uma competição entre três autores para ganhar o imaginário prêmio de quem teria utilizado pela primeira vez a expressão Sociedade da Informação e é quase impossível decidir qual foi a primeira publicação, em face das dificuldades de reconstrução temporal entre a preparação e a publicação dos ensaios.[196] Em seu trabalho, Tadao Umesao sustentava a mudança social mais centrada na informação e o fazia com analogia à evolução da natureza e na sequencia vieram outros trabalhos de autores japoneses e o fato é que muito rapidamente o termo foi levado ao Ocidente e adotado pela comunidade cientifica da Europa.

---

[194] DUFF, op. cit., p. 4-5.

[195] KARVALIC, op cit., p. 14.

[196] Confira-se: "Three authors are in competition to win the imaginary award for being the first to use the collocation "information society" in their book's title and due to the reconstruction difficulties in regard to the dates of preparation and publication of the manuscripts, it is almost impossible to decide which publication was the first: Yujiro Hayashi's bestseller of 1969 (Johoka Shakai: Hado No Shakai Kara Sofuto no Shakai e, The Information Society: From Hard to Soft Society) or the introductory and popularising books by Yoneji Masuda and Konichi Kohyma published in 1968 (Joho Shakai Nyumon - Introduction to an Information Society)." KARVALIC, op. cit., p. 14.

Ao assumir a vertente de ser um conceito ainda indefinido, os autores de uma forma geral buscam cada um dar um nome diferenciado, mas sem fugir ao cerne da discussão. Portanto, pode ser encontrados os termos Sociedade do Conhecimento, Sociedade Digital, Sociedade Rede e também a adoção do termo sociedade tecno-comunicacional, mas com o predomínio do uso da expressão Sociedade da Informação, cujo correlato econômico encontra-se na expressão nova economia ou economia digital.[197]

Paralelamente aos contornos científicos do termo Sociedade da Informações encontradas na literatura japonesa, nos Estados Unidos da América, alguns estudos já vislumbravam de forma didática as consequências econômicas em face da disseminação do conhecimento. Nessa linha, importante foram os trabalhos de Fritz Machlup, com a publicação de um influente estudo sobre a produção e distribuição do conhecimento na economia quando analisou a contribuição da indústria do conhecimento para o Produto Nacional Bruto daquele país.[198]

Catrin Pekari afirma que nos idos dos anos 70, quando da iminência das crises econômicas, os conceitos de mercado da Sociedade da Informação entendiam as novas tecnologias como um meio para aumentar a produtividade e promover maior competitividade. É de 1980 o livro a *terceira onda* (*The Third Wave*) obra amplamente comentada, quando em um exercício de futurologia Alvin Tofler, previu o impacto que

---

[197] Vide entre outros, AVANCINI, Helenara Braga. O paradoxo da sociedade da informação e os limites dos direitos autorais. In: ROVER, Aires José. (org). *Direito e informática*. Barueri, SP: Manole, 2004. p. 357; DRUMMOND, Victor. *Internet, privacidade e dados pessoais*. Rio de Janeiro: Lúmen Júris, 2003. p. 2; BALLESTEROS MOFFA, Luis Ángel. *La privacidad electrónica:* internet em el centro de protección. Valencia: Tirant L Lanch, 2005. p. 33 e SIMÃO FILHO, Adalberto. Sociedade da informação e seu lineamento jurídico. In: PAESANI, Liliana Minardi (coord). *O direito na sociedade da informação*. São Paulo: Atlas, 2007. p. 9.

[198] PEKARI, Catrin. The Information Society and its policy agenda: towards a human rights-based approach. *Revue Québécoise de Droit International*, v. 18, n. 1, 2005. p. 60. Disponível em: <https://www.sqdi.org/wp-content/uploads/18.1_-_pekari.pdf>. Acesso em: 29 abr. 2017. MACHLUPT, Fritz. 1962, apud PEKARI, Catrin. The Information Society and its policy agenda: Towards a human rights-based approach. *Revue Québécoise de Droit International*, v. 18, n. 1, 2005. p. 60. Disponível em: <https://www.sqdi.org/wp-content/uploads/18.1_-_pekari.pdf>. Acesso em: 29 abr. 2017.

PROGRAMA DE PÓS-GRADUAÇÃO MESTRADO PROFISSIONAL EM DIREITOS SOCIAIS E PROCESSOS REIVINDICATÓRIOS/PPGDIesb - ISSN: 2448-2358

as novas tecnologias que estavam surgindo causariam na nova economia, ao colocar no centro de todas as mudanças políticas, sociais, culturais e econômicas a ampla disseminação do computador, assim como foi com a pílula anticoncepcional, a aviação comercial com as viagens a jato e os avanços na agricultura e indústria em geral, o que denominou de *era da informação*.[199]

No seio da comunidade europeia os estudos foram avançando e o Conceito de Sociedade da Informação foi adotado naturalmente, a exemplo dos Livros Verdes da Sociedade da Informação. Em verdade, a adoção do conceito de Sociedade da Informação decorre de uma postura eminentemente política e pragmática, considerando os diversos documentos nos quais consta a exemplo dos conhecidos *Livros Verdes* (*Green Papers*).

A propósito, no Livro Verde do Brasil, é compreendido que a Sociedade da Informação não é um modismo, pois ao aceitar a globalização do fenômeno e a visão de que representaria, como de fato representa, uma profunda mudança na organização da sociedade, em particular da economia, ou seja, um "novo paradigma técnico econômico.[200] No livro verde de Portugal, a Sociedade da Informação a compreensão é de que

---

[199] Vide TOFFLER, Alvin. *A terceira onda*. Rio de Janeiro: Record, 1980. Alvin Toffler ensina que passamos por um período revolucionário que vai além da inovação tecnológica, da importância dos computadores e das telecomunicações, pois devemos reconhecer as alterações na economia, nas relações sociais, culturais, políticas, religiosas e institucionais. E vai além, estão acontecendo alterações filosóficas ou, "mais precisamente, epistemológicas." E prossegue, há o apontar de "a new way of life". Alvin Toffler chama esses períodos revolucionários de ondas, quando a primeira vez foi quando a raça humana passou de uma civilização tipicamente nômade para uma civilização basicamente agrícola, sedentária, o que ocorreu há cerca de 10 mil anos, na segunda vez foi quando a raça humana passou de sua civilização predominantemente agrícola para uma civilização basicamente industrial (há uns 300 anos, nos EUA e na Europa) e a terceira onda dessa revolução começou a acontecer por volta de 1955 nos Estados Unidos e em alguns outros países que estavam no auge do seu desenvolvimento industrial. Alvin Toffler, em *The Third Wave* chamou essas três revoluções de "ondas" e embora essa terceira onda tenha sido chamada por vários nomes (Sociedade Pós-Industrial, Sociedade da Informação, etc.), a melhor maneira de entendê-la é contrastando-a com a segunda onda, a era da civilização industrial. In: TOFFLER, Alvin. *Terceira onda*. Disponível em: <http://www.projeto.unisinos.br/humanismo/antropos/Terceira_Onda.pdf>. Acesso em: 19 ago. 2017.

[200] A SOCIEDADE da informação. *In:* TAKAHASHI, Tadao (Org.). *Sociedade da informação no Brasil*: livro

PROGRAMA DE PÓS-GRADUAÇÃO MESTRADO PROFISSIONAL EM DIREITOS SOCIAIS E PROCESSOS REIVINDICATÓRIOS/PPGDIesb - ISSN: 2448-2358

> refere-se a um modo de desenvolvimento social e económico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação conducente à criação de conhecimento e à satisfação das necessidades dos cidadãos e das empresas, desempenham um papel central na actividade económica, na criação de riqueza, na definição da qualidade de vida dos cidadãos e das suas práticas culturais (ICP/ANACOM).

A referência à Sociedade da Informação está tão patente, de forma tão intensa e continuada, que em geral todos a identificamos como uma etapa histórica vinculada à evolução tecnológica no entorno prévio à convergência dos meios de comunicação e informáticos permitiram, não somente oferecendo melhores serviços de telecomunicações ou de informática e novos resultados que incidem em grandes lucros para a ciência, a sociedade, a economia e o próprio direito, afirma Moro Almaraz (2004, p. 108). Sustenta Moro Almaraz, resta superado definir Sociedade da Informação, a qual deve ser compreendida como um resultado da autêntica revolução tecnológica provocada durante a década dos anos 90 e pelo desenvolvimento da informática, dos meios de comunicação, e da progressiva generalização do uso e utilização dos computadores pessoais e da Internet por empresas e particulares (*idem, ibidm*).

A propósito, Helenara Avancini (2004, p. 356) refere que o paradigma da sociedade da informação, em alusão a Internet e afirma que o mundo está vivendo a chamada Quarta Onda, notadamente pela valorização da informação, pois o objetivo da Sociedade da Informação é proporcionar o constante avanço nas infraestruturas globais da informação, propiciando, por meio de incentivos, o desenvolvimento das inovações tecnológicas.

Não há entre os autores um conceito estanque, e a Sociedade da Informação "antes de prestar a ser um elemento jurídico que possa dar origem a um segmento específico do direito, quando vista em razão de suas intercorrências, é um princípio de

---

verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Capítulo 1. p. 5.

natureza socioeconômico" (SIMÃO FILHO, 2007, p. 9). Destarte, é bem difundida a ideia de a Sociedade da Informação ser um espectro das tecnologias da informação e da comunicação, ai englobando a aquisição, armazenamento, processamento e distribuição da informação pelos meios eletrônicos.[201]

2 Sociedade da informação e a internet: a mescla de termos

O lado mais visível da Sociedade da Informação é a Internet e suas funcionalidades, e a fuga de um conceito hermético pode ser uma solução para evitar confusão no alcance multidisciplinar da disciplina, como destaca Simão Filho. [202] Ademais, Manuel Castells é preciso ao afirmar, a Internet é a sociedade, pois expressa processos sociais, interesses sociais, valores sociais e instituições sociais.[203] E em sua palestra, Manuel Castells questiona qual é então a especificidade da Internet? E sustenta a especificidade da Internet é que ela constitui a base tecnológica da rede da sociedade, a infraestrutura tecnológica e o ambiente organizacional, o que permite o desenvolvimento de uma série de novas formas de relações sociais. Essas novas formas

---

[201] Cfr. SIQUEIRA JR., Paulo Hamilton Siqueira. Direitos Humanos e cidadania digital. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. 1. p. 176.

[202] Cfr. SIQUEIRA JR., Paulo Hamilton Siqueira. Direitos Humanos e cidadania digital. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. 1. p. 13.

[203] Cf. CASTELLS, Manuel. *Internet e sociedade de rede:* Lliçó inaugural del programa de doctorat sobre la societat de la informació i el coneixement. Disponível em: <http://www.uoc.edu/web/cat/articles/castells/print.html>. Acesso em: 30 abr. 2017. Neste ensaio não há a pretensão de analisar as obras de Castells, mas é importante destacar o seu papel fundamental nos estudos dos desenvolvimentos da internet e da era da sociedade da informação.

de relações sociais são o resultado de uma série de mudanças históricas, as quais não teriam sido desenvolvidas sem a Internet.

Essa sociedade em rede, é a sociedade cuja estrutura social é construída em torno de redes de informação, de microeletrônica, da tecnologia, estruturadas de informações na Internet.[204] Mas a Internet, nesse sentido, não é apenas uma tecnologia; é o meio que é a forma de organização das nossas sociedades, é o equivalente do que foi outrora a fábrica na era industrial ou grande empresa na era industrial. Assim, a Internet é o coração de um novo paradigma sociotécnico que realmente constitui a base material de nossas vidas e nossas formas de relacionamento, trabalho e comunicação.[205]

Segundo Manuel Castells, a rede de Internet foi desenvolvida ao mesmo tempo, com a interação da investigação universitária básica, programas de pesquisa militar nos Estados Unidos e uma contracultura radical libertária. [206] E embora a origem da Internet fosse um programa de pesquisa militar, na prática nunca teve uma aplicação militar e os cientistas a usavam para fazer suas coisas, seus estudos de computador e também da rede tecnológica.

Ponto importante é que a Internet não foi criada como um projeto de lucro corporativo e quando o Pentágono tentou privatizar a ARPANET, o antepassado da Internet como é conhecida hoje, foi oferecida graciosamente em 1972 a grande empresa Americana de Telecomunicações, a ATT. A empresa estudou o assunto e afirmou que o projeto nunca seria rentável e não viu nenhum interesse em comercializá-lo.[207]

Para Manuel Castelis, a Internet não é apenas uma tecnologia, mas é o meio ou um meio que forma a organização da nossa sociedade, ou o equivalente ao que foi outrora a fábrica na era industrial ou às grandes empresas na era industrial. É a Internet

---

[204] Ibidem.
[205] Ibidem.
[206] Ibidem.
[207] CASTELLS, Manuel. *Internet e sociedade de rede:* lliçó inaugural del programa de doctorat sobre la societat de la informació i el coneixement. Disponível em: <http://www.uoc.edu/web/cat/articles/castells/print.html>. Acesso em: 30 abr. 2017.

o coração de um novo paradigma sócio-técnico que realmente constitui a base material de nossas vidas e nossas formas de relacionamento, trabalho e comunicação e assim torna-se a virtualidade para transformá-la em nossa realidade, constituindo a sociedade em rede, que é a sociedade em que vivemos.[208]

A Internet nasceu livre e assim deveria continuar, livre da interferência dos governos e de seus regulamentos. [209] Há uma corrente de pensamento, nominada como o "pensamento libertário" com a linha de dever ser garantida liberdade plena de expressão em seu meio, pois é um foro democrático no qual os indivíduos podem ser criadores de seu próprio meio e a rede é um meio de libertação de muitas das desigualdades da economia real.[210]

Por isso, a Internet é o elemento-chave da chamada Sociedade da Informação, além de facilitar os mais variados serviços eletrônicos interativos e a comunicação de todo tipo de informações (texto, som, imagens, vídeo, programas e outros tipos de dados).

3 A era da internet das coisas

É em uma fase mais atualizada da era da Internet, a Internet das coisas foi identificada como a terceira onda da Internet e cada vez mais há dispositivos domésticos conectados em redes de internet sem fio (wifi) e esses dispositivos controlam todos os nossos passos. Os dispositivos (as coisas) sabem quando brincamos, dormimos, como e onde trabalhamos, se usamos ou não medicamentos (lícitos ou

---

[208] Ibidem.

[209] Para o assunto, Vide, *Reno v. American Civil Liberties Union*. 521 U.S. 844 (1997). Nesse julgamento, os juízes da Suprema Corte americana enfatizaram a necessidade de a Internet ser protegida contra as indevidas tentativas de uma regulação estatal desvirtuando suas características essenciais, entre elas, a interatividade e a impossibilidade técnica de exercer filtros prévios aos materiais que seriam disponibilizados aos internautas.

[210] Cfr. LORENZETTI, Ricardo L. *Comércio eletrônico*. Notas de Cláudia Lima Marques. São Paulo: Revista dos Tribunais, 2004. p. 71.

ilícitos), ou seja, a nossa rotina é permanentemente monitorada e há a capacidade técnica de coleta e de troca de dados sobre praticamente todos os aspectos da nossa privacidade e de nossos negócios.

A *IDC* (ou *IoT*, na expressão utilizada em língua inglesa) é um conceito que representa a rede de dispositivos inteligentes (ou "coisas") que estão conectados à internet e uns aos outros e têm a capacidade de coletar e de trocar os dados sobre todos os aspectos de nossos negócios e de nossas vidas, queiramos ou não. A *IDC* é um conceito que está relacionado da forma como há a interação entre os computadores, sensores e os objetos interagem uns com os outros e passam a coletar as diversas informações relacionadas ao ambiente [211], e de que modo essas tecnologias interconectadas podem contribuir com a vida cotidiana das pessoas, tornando-a mais fácil, notadamente em sua organização.

A IdC/IoT permite que os dispositivos se conectem à Internet por meio de sensores incorporados nos dispositivos os quais enviam informações do ambiente para centros de armazenamento de dados, onde podem ser tratados para fins de controle e de feedback. A IdC/IoT transformou os dispositivos do dia-a-dia em dispositivos inteligentes conectando objetos de consumo e equipamentos industriais à Internet, permitindo a coleta e o gerenciamento de informações desses dispositivos por meio de

[211] Não existe uma definição única disponível para a *Internet of Things* e aceitável pela comunidade mundial de usuários e em variados grupos, entre acadêmicos, pesquisadores, profissionais, inovadores, desenvolvedores e pessoas corporativas que definiram o termo, embora seu uso inicial tenha sido atribuído a Kevin Ashton. Para maiores desenvolvimentos, *vide* MADAKAM, Somayya; RAMASWAMY, R; TRIPATHI, Siddharth. Internet of Things (IoT): a literature review. *Journal of Computer and Communications*, 2015, 3, 164-173. Published Online May 2015 in SciRes. Disponível em <http://www.scirp.org/journal/jcc http://dx.doi.org/10.4236/jcc.2015.35021>. Acesso em: 17 abr. 2018. p. 165. Sob o ponto de vista jurídico, ocorre o impasse do Direito ante o fato da globalização. Torna-se necessário estabelecer, refere Liliana Minardi Paesani, que o Direito é uma ciência de segundo grau e, como tal, depende do conhecimento da realidade a que se refere. Portanto, não basta conhecer a norma, é indispensável conhecer preliminarmente o fenômeno que se quer disciplinar por meio da lei, estudar as situações concretas em que será aplicada e prever s efeitos que surgirão da interação entre a situação de fato e o preceito normativo. In: PAESANI. *Direito e internet:* liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2003, p. 18.

software para aumentar a eficiência, possibilitar novos serviços ou obter outros benefícios ambientais, entre os quais de mecanismos mais eficientes de segurança.[212]

A literatura é farta para ilustrar as diversas funcionalidades existentes da Internet das Coisas. A lista de coisas conectadas em Internet é infindável. Vejamos alguns exemplos:

a) há dispositivos que permitem o monitoramento remoto de crianças e de bebês; b) dispositivos para ajudá-lo a lembrar de tomar seus medicamentos; c) dispositivos para rastrear seus níveis de atividade; d) dispositivos para ajudar a monitorar um membro idoso da família; dispositivos médicos que permitem que sua saúde seja monitorada por seu médico e que automaticamente libere níveis adequados de medicação; e) dispositivos que permitem monitorar remotamente sua casa; dispositivos que permitem desligar aparelhos ou alterar a temperatura em sua casa; f) há aparelhos de ar condicionado com possibilidade de conexão com a internet; g) dispositivos que permitem alimentar e regar suas plantas e animais de estimação; h) há geladeiras que lembram até mesmo quando vamos ficar sem cerveja; i) há as TVS "inteligentes ou espertas" e até mesmo brinquedos sexuais conectados em Internet; j) Ainda, há dispositivos que permitem o monitoramento da coleta do lixo, os fluxos de tráfego, os níveis de poluição, o uso de eletricidade e a solidez estrutural de edifícios e estradas; e l) Há dispositivos que permitem às empresas monitorar as necessidades de reparo e manutenção de equipamentos e acompanhar as tendências de marketing em tempo real nas lojas.[213]

---

[212] O'BRIEN, Michael H. *The internet of things*: the inevitable collision with product liability. Disponível em: <https://www.productliabilityadvocate.com/2015/02/the-internet-of-things-the-inevitable-collision-with-product-liability/>. Acesso em: 17 ab. 2018. Postado em: 2 fev. 2015.

[213] Para esse desenvolvimento, *vide* GORMAN, Leta E. The era of the internet of things: can product liability laws keep up?. *Defense Counsel Journal*, v. 84, n. 3. Disponível em: <https://www.iadclaw.org/publications-news/defensecounseljournal/the-era-of-the-internet-of-things-can-product-liability-laws-keep-up/> Acesso em: 17 abr. 2018.

O vertiginoso crescimento da internet das coisas é irrefutável. Alguns apontamentos indicam que até 2020 possam existir cerca de 50 bilhões de dispositivos conectados em rede, com a consequência de muito mais dados serão gerados, o que deve exceder os quinze *exabytes*, ou seja, cerca de 15 quintilhões de *bytes* a cada mês.[214] Os benefícios obtidos com a conexão das coisas na internet certamente é um ponto importante para explicar o crescimento vertiginoso de sua utilização e também explica o rápido surgimento de aplicativos tornando cada dia mais funcional a conexão entre coisas, pessoas e o ambiente virtual.

Ao passo que há enormes benefícios, por outro lado temos que pensar na possibilidade da potencialização de danos, tais como os riscos de segurança, tanto de pessoas como de instalações físicas, da violação da privacidade e da exposição de dados, entre tantos outros riscos. Por riscos de segurança, deve ser pensado no risco inerente da invasão e tomada do controle de um dispositivo conectado em rede de Internet.

Ora, imagine a seguinte situação: o sistema de aquecimento de água em uma residência, controlado por um software é invadido por hackers, os quais aquecem a água remotamente a níveis absurdos com a capacidade de causar danos físicos aos usuários ou os sistemas de segurança de uma residência são invadidos e acionam o alarme de suposta invasão por uma madrugada inteira, causando perturbação no sossego alheio, além de atrair indevidamente o aparato a segurança pública ou configurar um elemento de facilitação de furtos e de roubos. E hipoteticamente, há a possibilidade de danos muito mais graves, como da ideia do fornecimento de medicamentos remotamente e de modo automático, quando o paciente pode deixar de receber a dose necessária ou até mesmo ser inoculado à distância com uma dose letal,

---

[214] GORMAN, Leta E. The era of the internet of things: can product liability laws keep up?. *Defense Counsel Journal*, v. 84, n. 3. Disponível em: <https://www.iadclaw.org/publications-news/defensecounseljournal/the-era-of-the-internet-of-things-can-product-liability-laws-keep-up/> Acesso em: 17 abr. 2018. Para comparar, de acordo com uma estimativa, um *exabyte* de armazenamento poderia conter 50.000 anos de vídeo com qualidade de DVD.

PROGRAMA DE PÓS-GRADUAÇÃO MESTRADO PROFISSIONAL EM DIREITOS SOCIAIS E PROCESSOS REIVINDICATÓRIOS/PPGDIesb - ISSN: 2448-2358

por ato deliberado de um cracker ou por uma falha no sistema informático que alimenta o dispositivo com informações em tempo real e à distância.

Também há enormes riscos, não somente causados pelos tradicionais provedores de serviços de Internet, como representativos da maior ameaça à privacidade[215], temos ainda de compreender que os dispositivos conectados em rede coletam, armazenam e transmitem dados pessoais dos consumidores.[216] Vez por outro são noticiados casos de vazamento de dados contidos em bancos de dados de importantes prestadores de serviços de aplicativos de transporte de passageiros, da invasão de bancos de dados de empresas que atuam principalmente no mercado eletrônico e até mesmo na captura de dados pessoais de usuários da plataforma da rede social do facebook.

Há mesmo a franca possibilidade de uma televisão esperta ou inteligente (*smart*) ser controlada à distância por seus desenvolvedores ou por piratas da Internet, com o grave comprometimento de informações pessoais, informações que podem ser vendidas, compartilhadas e usadas para fins ilícitos e já se falou até mesmo da possibilidade de conversas privadas ser expostas.[217]

---

[215] OHM, Paul. *The Rise and Fall of ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1417. O referido autor refere em seu ensaio que as atividades dos *ISP* (*Internet Service Provider*), representa uma grave ameaça à privacidade, dado que transmitem as conversas, segredos, relacionamentos, atos e omissões de seus usuários e vão além, pois possuem arsenal tecnológico para uma espionagem invasiva, de formas sem precedentes, o que foi facilmente percebido pelos interesses dos anunciantes em saber dos interesses dos usuários. No ensaio, o articulista propõe aos formuladores de políticas a distinguir entre os interesses legítimos dos provedores dos meros desejos e ainda tece considerações sobre a neutralidade da rede - um debate sobre quem controla a inovação na Internet.

[216] OHM, Paul. *The Rise and Fall of ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1417.

[217] SAMSUNG adverte: cuidado com o que você diz em frente a sua TV inteligente. *O Globo*, 9 maio 2015. Disponível em <https://oglobo.globo.com/sociedade/tecnologia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181>. Acesso em: 17 abr. 2018. No que tange a ataques contra as Smart TVs, o fato já é uma realidade e não há a necessidade de acesso físico ao aparelho ou qualquer interação com o usuário. Estudos apontam que é possível ativar, por exemplo, a câmera e o microfone internos remotamente. E não só eles poderiam transformar essas TVs em dispositivos capazes de ouvir e observar, mas também poderiam assumir o controle de aplicativos de redes sociais incorporados para publicar informações em nome do usuário e acessar arquivos. In: IDGNOW. *Fique atento, sua Smart TV pode estar espionando você e sua família*. Disponível em: <http://idgnow.com.br/ti-

4 Problemas suscitados com a internet das coisas

Com a ampla disseminação da utilização da Internet, não tardou o surgimento ou o recrudescimento de uma variedade de problemas jurídicos com o uso das funcionalidades da rede. No campo da *IDC*, entre tantos problemas possíveis, e alguns referidos de passagem, cabe destacar a acentuada erosão da privacidade, da intimidade, da honra, da imagem, da coleta e tratamento de dados, sensíveis ou não, dada às amplas possibilidades de engenharia social[218], da invasão de sistemas informáticos e de sites de internet, das fraudes bancárias etc.

A quem imputar a responsabilidade civil ou penal pela violação de Direitos protegidos? Por outro lado, como proteger o consumidor (usuário) da Internet em face da necessidade econômica dos prestadores de serviços em internet com a lucratividade inerente ao capitalismo? O desenho de responsabilidade objetiva do Código de Defesa do Consumidor pode ser transposto automaticamente aos problemas suscitados nas ocorrências da internet das coisas? O fabricante e o importador podem ser

---

pessoal/2018/04/22/fique-atento-sua-smart-tv-pode-estar-espionando-voce-e-sua-familia/>. Acesso em: 9 maio 2018.

[218] Entenda-se por engenharia social como um método de ataque em que uma pessoa mal-intencionada faz uso da manipulação psicológica para induzir alguém a fazer ações específicas, como divulgar informações pessoais, baixar aplicativos falsos ou abrir links maliciosos. Diferente dos ataques de hacking tradicionais, a engenharia social não faz uso de sistemas sofisticados ou softwares de última geração. No meio digital, a engenharia social pode ser feita através de envio de e-mails, mensagens instantâneas, perfis falsos nas redes sociais ou até mesmo por chamadas telefônicas. Ao entrar em contato com a vítima, independente do modo, o criminoso tenta ganhar sua confiança para obter informações pessoais e credenciais, com o objetivo de realizar fraudes. Confira-se o texto completo In: PAVÃO, Samantha. **Tudo o que você precisa saber sobre engenharia social.** Postado em: 26 jan. 2018. Disponível em: <https://www.psafe.com/blog/o-que-e-engenharia-social/>. Acesso em: 9 maio 2018. É possível, por exemplo, obter dados cadastrais armazenados em algum detentor de dados e enviar e-mails como se fosse o próprio controlador desses dados e enganar as vítimas, causando-lhe outros prejuízos, além da mera captação ilícita dos dados que estavam armazenados e por falha na segurança foram invadidos. As notícias de recentes invasões de dados pessoais, como nome, endereço, CPF e conta de e-mail de grandes empresas que atuam no mercado eletrônico geram esse tipo de preocupação e há a necessidade de aferir qual o grau de responsabilidade das empresas e eventual excludente ou não do dever de indenizar, em face do fato de terceiro.

responsabilizados pelos causados aos usuários (consumidor) e terceiros afetados (consumidor vítima de um acidente de consumo)? Em quais situações? O fornecimento de produtos e serviços com a possibilidade de conexão à internet das coisas é uma atividade de risco para os direitos de outrem na dicção do parágrafo único do art. 927, do Código Civil ou é a típica responsabilidade objetiva de que trata o art. 931, do CC (produtos postos em circulação)? E as excludentes do dever jurídico de indenizar, como devem ser aplicadas?

Para oferecer alguma contribuição na solução de casos que devem surgir na seara dos tribunais brasileiros, é interessante trazer à colação problemas reais em discussão nos Estados Unidos e como poderia ser solucionado com base no nosso ordenamento jurídico. O fenômeno da globalização e a natureza da internet não mais permitem soluções únicas, em desconformidade com o resto do mundo e para tanto, ao intérprete deve ser buscado o amparo das armas que a legislação posta lhe oferece, ou na preciosa lição de Manuel Carneiro da Frada, o cuidado de procurar a solução "no tesouro da dogmática comum da imputação de danos" (FRADA, 2001, p. 7).

5 Noções de dados e a tutela pelo direito

Na compreensão do que deve cuidar o Direito, a primeira ideia é a de responder algumas questões prévias, a exemplo do que são dados protegidos sob o nosso ordenamento jurídico, afinal quais dados não podem ser objeto de recolha, de tratamento e de reversão do processo de anonimização. No mesmo sentido, há algumas categorias de dados que podem ser e como devem ser tutelados pelo Direito? O sistema legal brasileiro pode responder satisfatoriamente das amplas possibilidades de uso ilícito de dados disponibilizados ao público em geral por empresas detentoras desses dados, mesmo com a anonimização desses dados? O amplo leque imaginado das graves questões de engenharia social, já delineado anteriormente, não merece proteção da ordem jurídica? É um território ou espaço sem proteção?

De início, no estreito campo de investigação deste ensaio, compreendemos os dados pessoais como aqueles relacionados a pessoas individualizadas ou com possibilidade de ser individualizada, direta ou indiretamente e merece a tutela jurídica, pois em alguma partida susceptível de causar dano a direitos da personalidade, notadamente no campo da privacidade. Alguns desses dados, além da categorização de dados pessoais, ainda há o que se convenciona de denominá-los de dados de natureza sensível, ou seja, não deveria ser admitido qualquer possibilidade de tratamento, posto que são dados referentes aos aspectos mais íntimos de um sujeito, como convicções sexuais, religiosas, políticas ou filosóficas.

Após a edição da Lei do Marco Civil da Internet (Lei 12.965), com o escopo de regulamentá-la, veio a lume o Decreto 8.771, de 11 de maio de 2016, praticamente o último ato do Governo da então Presidente Dilma Rousseff. Esse decreto delineou que dado pessoal é o dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa. O Decreto esclarece que tratamento de dados pessoais é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Quando o usuário de Internet acede ao meio, recebe a sua identificação por meio do chamado IP, ou seja, o endereço de protocolo de internet que é o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais, na dicção da Lei 12.965/2014, art. 5, inciso III), dado numérico que em tese pode identificar um determinado usuário que acedeu a alguma coisa disponível na rede de Internet. Esse dado identificador do usuário é um dado pessoal a merecer o amparo da ordem jurídica? Ao comparar a atual legislação da Comunidade

Europeia com alguns textos legais do Brasil, pode ser afirmado, o endereço IP do usuário de internet configura um dado pessoal. [219]

A propósito, mais adiante vamos retornar ao tema, a Lei Geral de Proteção de Dados (LGPD), embora ainda não esteja em vigor, considera como dado pessoal a informação relacionada a pessoa natural identificada ou identificável. Dessa forma, o endereço IP poderá ser interpretado como um dado relacionado a uma pessoa natural identificável, dada a ampla possibilidade de ser identificado o usuário da Internet pela recolha dos dados do acesso à rede.

6 Estudo de casos dos estados unidos da américa

Nos Estados Unidos da América, já há casos antigos que trataram sobre a coleta de dados, notadamente para discutir a privacidade em matéria de fluxo dos dados, como foi o caso do *FTC* v. *GeoCitites* (1998) e mais recentemente alguns relacionados aos dados pessoais coletados pela *Google*. Esses casos não serão tratados aqui, pois dizem

[219] Tem ocorrido um debate entre os defensores da privacidade na Europa, de que os endereços IP merecem a qualificação de "dados pessoais", sob o manto da Diretiva de Proteção de Dados, com alguma divisão nos tribunais de Estados Membros, com reconhecimento na Suécia e Espanha, enquanto na França, Alemanha e Reino Unido não pode ser considerado como dado pessoal e assim, estar no escopo das regras da Diretiva e atual regulamento. As empresas que fornecem mecanismos de buscas, a exemplo da Google, sustentam a não aplicabilidade da Diretiva, pois somente os dados que puderem ser vinculados a um único ser humano pelo administrador de dados podem assim ser compreendidos, além de a empresa apenas disponibilizar parte dos números do endereço IP. O argumento da Google não é consistente, dado que há meios técnicos de identificar o usuário de um número IP e de seu núcleo familiar. Além disso, a Google colaciona os endereços IPs de seus usuários, armazenados e conectados à identidade e ao comportamento revelado pelas buscas e as empresas que prestam os serviços de internet à cabo e telefone mantêm bancos de dados que são associados a endereços IP diretamente com os nomes, endereços e números de cartão de crédito. Para maiores desenvolvimentos acerca do afirmado, *vide* OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, 2010. p. 1772-1774. O autor referido sustenta, mais adiante em seu ensaio, que os argumentos da Google não passam de exagero e de evasivas legais, pois a divulgação parcial dos números do IP, de apenas quatro octetos, com as informações externas colidas em outras fontes, permitem a reindentificação do usuário do serviço da empresa. Em suma, a empresa *Google* não merece nenhum crédito pela exclusão parcial de endereço IP, pois não fez quase nada para reduzir o risco de identificar o usuário e os modelos regulatórios deveriam pedir, no mínimo, o descarte de todos os endereços IP associados a pesquisa, o que já vem sendo feito pela buscador da Microsoft e da Yahoo!. Ibidem, p. 1774.

respeito às questões basilares da internet. O presente artigo é mais restrito, pois a abordagem é pertinente às questões da Internet das coisas, com estudo de casos reais objeto de debate judicial nos Estados Unidos da América.

6.1 O caso das TVs inteligentes

Em uma ação proposta pela Comissão Federal de Comércio (ou *Federal Trade Comission* – FTC) e o procurador geral de New Jersey em face da empresa VIZIO, conhecida empresa fabricante de Televisão foi sustentado que ocorreu a recolha e compartilhamento de dados dos consumidores, sem aviso e sem consentimento.[220]

O fato é que a fabricante, empresa estabelecida nos Estados Unidos da América, comercializou depois de 2010 mais de 11 milhões de televisões, com conexão à Internet e desde 2014, os seus aparelhos podem monitorar continuamente o que os consumidores assistem e essa informação é recolhida e transmitida por meio de um software de reconhecimento, o *ACR*. As televisões comercializadas a partir de 2014 já vinham com essa função ativa e os antigos aparelhos foram atualizados remotamente com essa função. Por meio do ACR, as televisões da VIZIO transmitem informações sobre o que um consumidor está observando em uma base segundo a segundo e captura as informações sobre uma seleção de pixels na tela e envia esses dados para os servidores da empresa, comparando com uma base de dados de conteúdos de programação de televisão, filmes e de natureza comercial, o que permitia a empresa saber exatamente o que os consumidores assistiam em um determinado momento.

[220] Explica Guilherme Guidi: "As condições e características desse consentimento variam de acordo com o setor de mercado e com a corte competente, mas é bastante claro que o consentimento possui, no contexto norte-americano, valor muito maior que aquele a ele atribuído nos demais modelos regulatórios, pois não se trata aqui de um *consentimento informado*, livre ou expresso, *resultado da consideração do indivíduo sobre o que se pretende com seus dados* e o sopesamento entre benefícios e malefícios. O consentimento, na tradição norte- americana, parece ter maior ligação com a *venda* de informações que com o estabelecimento de uma relação entre o usuário e o responsável pelo tratamento, dando-se ao contrato o tom de uma transação comercial, ao invés de uma cessão temporária de direitos sobre os dados em questão." GUIDI, Guilherme Berti de Campos. *Modelos regulatórios para proteção de dados pessoais*. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 3 abr. 2019.

PROGRAMA DE PÓS-GRADUAÇÃO MESTRADO PROFISSIONAL EM DIREITOS SOCIAIS E PROCESSOS REIVINDICATÓRIOS/PPGDIesb - ISSN: 2448-2358

Os aparelhos de TV da VIZIO coletam os dados de exibição das operadoras de TV de serviços por cabo e de internet de banda larga, inclusive com leitura dos DVD e é possível que o *ACR* possa captar até 100 bilhões de pontos de dados a cada dia de mais de 10 milhões de televisores VIZIO e esses dados podem ser armazenados indefinidamente. O software ACR da VIZIO também coleta periodicamente outras informações sobre a televisão, incluindo os endereços de IP, os endereços MAC com fio e sem fio, a força do sinal WiFi, os pontos de acesso Wi-Fi mais próximos e outros itens.[221]

A VIZIO monetiza os dados colhidos de seus consumidores mediante o fornecimento do histórico de visualização de televisão dos consumidores a parceiros comerciais mediante acordos de licenciamento, para três usos principais: desde ao menos o mês de maio de 2014 a VIZIO teria fornecido os dados de visualização dos consumidores a terceiros para fins de mensuração da audiência, ou seja, para determinar, no conjunto, o que os consumidores observam e como eles o observam. A VIZIO forneceu aos seus parceiros comerciais um identificador persistente para cada televisão (exclusivo para cada terceiro/parceiro comercial), em conjunto com o conteúdo (programas e comerciais) vistos, o momento da visualização, o tempo de visualização e os canais vistos. A VIZIO desde maio de 2015 teria fornecido os dados de

[221] O Instituto Brasileiro de Opinião Pública e Estatística, mais conhecido como IBOPE, é um dos grandes responsáveis por realizar a pesquisa e repassar os dados às emissoras de TV. Uma das formas que o instituto utiliza para coletar os dados dos usuários envolve um aparelho (*Peoplemeter*) que, instalado nas TVs de diversas residências, envia informações diárias ao IBOPE sobre os canais assistidos. Para que o instituto recolha os dados, é preciso que o *Peoplemeter*, seja ativado pelo usuário, mediante uma senha e o aparelho registra as preferências de cada morador no domicílio. Com isso, o Instituto consegue gerar relatórios aprofundados com relação às preferências de cada faixa etária nos diversos lares onde o aparelho está instalado. Entretanto, nem todo domicílio pode ser escolhido para participar da pesquisa de audiência. O IBOPE realiza uma espécie de mini censo, onde é realizado um estudo socioeconômico para selecionar adequadamente os domicílios que melhor representam o conjunto de residências em situação semelhante daquela região. As famílias que participam dessa avaliação não são remuneradas e precisam concordar com um contrato de sigilo sobre o uso do aparelho (*peoplemeter*). Para se ter uma ideia, na cidade de São Paulo existem 760 aparelhos. Já no Brasil, são 3.765 aparelhos espalhados por 14 cidades, principalmente capitais. In: RODRIGUES, Leonardo. Como se mede a audiência da TV aberta. *Tech Tudo*. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/07/como-se-mede-a-audiencia-da-tv-aberta.html >. Acesso em: 2 maio 2018.

visualização dos consumidores a terceiros para analisar a eficácia dos anúncios publicitários, mediante um programa de análise de dados. A VIZIO fornece aos seus parceiros comerciais os endereços IP, de modo que possam analisar o comportamento de uma família em dispositivos, a fim de determinar, por exemplo, (a) se um consumidor visitou um determinado site após um anúncio de televisão relacionado a esse site, ou (b) se um consumidor viu um programa de televisão específico após a exposição a um anúncio on-line desse programa. Os dados utilizados são tratados para avaliar a eficácia das campanhas publicitárias. Ainda, a VIZIO pode ter coletado e fornecido os dados de seus consumidores a terceiros com o objetivo de direcionar publicidade a consumidores específicos em seus outros dispositivos digitais com base em seus dados de exibição de televisão.

Por essas práticas da VIZIO, há a facilitação e possibilidade do fornecimento de informações demográficas a terceiros sobre os telespectadores das TV, pois os dados dos IP podem ser tratados em uma base de dados e com isso identificar um consumidor ou vincular a uma família específica e, em seguida, envia aos parceiros comerciais as informações demográficas associadas com a pessoa ou núcleo familiar. Os contratos da VIZIO com seus parceiros comerciais proíbem a identificação dos consumidores e das famílias pelo nome, mas permitem que as seguintes informações sejam colhidas: o sexo, a idade, a renda, o estado civil, o tamanho da família, o grau de educação, se a casa é propriedade própria ou eventuais dívidas.

A VIZIO declara que seu programa de análise de dados, por exemplo, "fornece dados de comportamento de visualização altamente específicos em larga escala e grande precisão, que podem ser usados para gerar informações inteligentes para anunciantes e provedores de conteúdo de mídia. No caso daqueles consumidores que adquiriram as novas televisões a partir de 2014, o sistema ACR vinha previamente instalado, sem qualquer informação de sua existência e no caso daqueles aparelhos anteriores, o sistema de rastreamento foi instalado remotamente, sem qualquer aviso em tempo suficiente para sua compreensão, eis que um pop-up com o aviso aparecia na

tela dando conta de alteração na privacidade, mensagem que expirava em menos de um minuto, não permitindo ao usuário obter com clareza de que poderia desativá-lo nas configurações.

Em março de 2016, já sob investigação da FTC e do Procurador Geral de New Jersey, as televisões da VIZIO passaram a exibir um aviso em pop-up que, pela primeira vez, referiam a coleção de dados de exibição de televisão. O aviso expirou após 30 segundos sem a entrada específica de qual membro do conjunto familiar que estava a ver a tela no momento, e não forneceu acesso fácil ao menu de configurações. Em todas as televisões habilitadas com rastreamento ACR, as TVs VIZIO tinham uma configuração disponível no menu de configurações, chamado "Interatividade inteligente". Esta configuração incluiu a descrição: "Possibilita ofertas e sugestões de programas". Da mesma forma, no manual para alguns aparelhos da VIZIO, uma seção intitulada "Interatividade inteligente" descrevia a prática como "Sua TV pode exibir informações relacionadas ao programa como parte da transmissão". Nenhuma descrição forneceu informações sobre a coleta de dados de visualização. A VIZIO não forneceu "ofertas ou sugestões de programas" ou "informações relacionadas ao programa" para a maioria das televisões por mais de dois anos e não atualizaram as divulgações.

Em resumo, as TVs da VIZIO poderiam infringir o sistema de proteção da privacidade nos Estados Unidos por fornecer os softwares de monitoração e compartilhamento dos dados dos consumidores, com ativação de padrão do fabricante e ativação remota pelo fabricante de produtos comercializados anteriormente, sem informações suficientes e claras da opção de consentimento prévio e informado do consumidor, notadamente às questões de Geolocalização.

O caso foi solucionado por acordo e a VIZIO, sem admitir as acusações, concordou em pagar uma multa de U$ 3.200.000 e U$ 300.000 suspensos, desde que cumpra com as regras estabelecidas. Desse modo, a VIZIO concordou em apagar todos

os dados coletados e do compromisso de obter o consentimento pelos consumidores, mediante avisos claros e ostensivos e de modo afirmativo. [222]

A questão que surge imediatamente neste mundo globalizado é se apenas a TV Vizio teria a capacidade de tal coleta e se as demais TVs no mercado, do padrão Smart também não são equipadas com tal capacidade de invasão na privacidade de seus consumidores? Cabe referir que já foi divulgado a possível violação da privacidade dos consumidores pelas TVs da SAMSUNG, em que os aparelhos poderiam gravar conversar travadas no ambiente e transmitir para um centro de armazenamento, embora a empresa negue do vazamento dos dados.[223]

6.2. Do brinquedo sexual ativado via bluetooth

Em um caso aparentemente jocoso, há uma *class action*, proposta em face da Hytto, Ltd. d/b/a Lovense. [224] A ação de classe sustenta que a empresa comercializa um objeto de natureza sexual (vibrador), objeto que pode ser ativado remotamente via função de bluetooth, desde que o usuário baixe o aplicativo da Internet e o use com seu smartphone. É sustentado na ação que a empresa e seus parceiros comerciais podem obter os dados de utilização do objeto em causa, pois a

---

[222] Para uma leitura do acordo firmado, *vide* em https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf. A VIZIO, ainda, em um acordo firmado, está pagando 16 milhões de dólares aos consumidores, ou seja, cerca de 1 dólar por consumidor que foi espionado, muito embora a empresa negue a prática ou que fosse ilegal.

[223] SAMSUNG adverte: Cuidado com o que você diz em frente a sua TV inteligente. O Globo, 9 maio 2015. Disponível em: <https://oglobo.globo.com/economia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181>. Acesso em: 3 abr. 2019.

[224] S.D. v. Hytto Ltd., d/b/a/ Lovense Plaintiff: S.D. Defendant: Hytto Ltd., d/b/a/ Lovense Case Number: 3:2018cv00688; Filed: January 31, 2018 Court: California Northern District Court Office: Oakland Office County: San Francisco Presiding Judge: Jeffrey S. White Nature of Suit: Other Statutory Actions Cause of Action: 28:1331 Jury Demanded By: Plaintiff.A inicial está disponível em < https://www.courthousenews.com/wp-content/uploads/2018/01/Lovense.pdf>. Acesso em 25 abril 2018. Case 3:18-cv-00688-MEJ Document 1 Filed 01/31/18 Page 1 of 14. Para acessar a home page da empresa, consulte <https://pt.lovense.com/bluetooth-remote-control-vibrator>.

empresa consegue operar remotamente e saber a frequência com que os brinquedos sexuais são utilizados e a intensidade de seu uso. Em suma, há aparentemente uma indevida violação da privacidade.

A empresa usa o aplicativo para coletar e registrar dados altamente íntimos e sensíveis sobre o uso pessoal dos consumidores de seus vibradores Lovense, incluindo a data e hora de cada uso e as configurações de vibração selecionadas e transmite a informação juntamente com o endereço de e-mail pessoal do usuário para seus servidores. O que está em debate é se há o conhecimento prévio e adequado de seus clientes, mediante informações claras.

O que a empresa fabricante sustenta é de que as políticas de privacidade já apontam a prova da autorização, pois assim dispõe: "Os usuários do nosso software e dos aplicativos devem concordar com nossa política de privacidade antes de usar nossos serviços. Ele menciona claramente o tipo de dados que transitam por nossos servidores".

6.3 Das falhas de segurança em software de automóveis.

Para o Direito norte americano, a responsabilidade do fabricante por defeitos de software não é nenhuma novidade, como foi relatado o caso de um homem que processou a General Motors em razão de um chip com defeito que foi causa suficiente para dar pane no motor do veículo o que fez com que parasse no meio de um cruzamento e foi atropelado por um trator, causando a morte de seu neto.[225]

Vejamos alguns casos mais recentes:

[225] Confira-se em Gen. Motors Corp. v. Johnston, 592 So. 2d 1054 (Ala. 1992). Apud BUTLER, Alan. *Products liability and the internet of (insecure) things*: should manufacturers be liable for damage caused by hacked devices?, 50 U. Mich. J. L. Reform 913 (2017). p. 925. Disponível em: <http://repository.law.umich.edu/mjlr/vol50/iss4/3>. Acesso em: 10 abr. 2018.

No caso conhecido por *Cahen v. Toyota Motor Corp.*, foi ajuizada uma *class action* contra a Toyota, a Ford e a General Motors, sob a alegação de a tecnologia computadorizada dos veículos ser vulnerável a ataque de hackers. Os autores alegaram a) um hacker pode se comunicar remotamente (através de Bluetooth ou celular) com os computadores dos veículos; b) após, pode passar a controlar diversas funções dos veículos, tais como o sistema de aceleração, frenagem e direção; d) do controle exercido sob os veículos, danos diversos poderiam ocorrer: e) os danos em potencial são do conhecimento das montadoras e mesmo assim os anúncios publicitários divulgavam os produtos como seguros.

Contudo, o processo não prosperou, pois, o juiz concordou com a defesa, no sentido de que há apenas um risco em potencial de uma futura invasão por hackers, o que não é propriamente uma lesão de fato e nem foi demonstrado qualquer ocorrência documentada de *recall* ao caso específico. [226]

Em um processo semelhante, em desta vez contra a *Chrysler Group*, em *Flynn v. FCA US LLC*, a alegação era de falha na central de entretenimento. A central poderia ser hackeada e controlada remotamente. Contudo, a Corte não admitiu a ação, sob o fundamento hipotético de danos futuros, mas aceitou que poderia existir redução no valor do veículo no mercado em razão das vulnerabilidades apontadas.

Desses casos de veículos, com base em supostas falhas na tecnologia com possibilidade de ser invadida por hackers, as cortes não admitem a demanda com base apenas na presunção de possível invasão.

6.4 Violação de segurança das "coisas" conectadas à Internet

[226] Conforme relatado, os autores apelaram da decisão que rejeitou a ação e o caso será julgado pelo 9º. Circuito Federal. Confira-se, in GORMAN, Leta E. The era of the internet of things: can product liability laws keep up? *Defense Counsel Journal*, v. 84, n. 3. Disponível em: <https://www.iadclaw.org/publications-news/defensecounseljournal/the-era-of-the-internet-of-things-can-product-liability-laws-keep-up/> Acesso em: 17 abr. 2018.

A questão de dispositivos inseguros representa uma ameaça significativa à segurança da internet, dada a possibilidade de "coisas" conectadas em rede ser utilizadas para destruir ativos digitais e a toda uma infraestrutura de rede de Internet e em particular, para a população em geral no sentido de causar danos tremendos a bens e a pessoas.

No dia 20 de setembro de 2016, o site KrebsOnSecurity, foi atingido por um grande ataque cibernético de negação de serviço ("DoS") e forçado a permanecer offline por vários dias após o seu provedor de segurança de rede ter recusado a continuar protegê-lo *pro bono*. Este ataque foi considerado um dos maiores já vistos por diversos fatores, entre eles o de que foi realizado por um exército de mais de um milhão de dispositivos hackeados e seguido de outro ataque poucos dias após, com a interrupção do acesso à Internet em toda a costa leste e em outras áreas dos EUA, com o registro de um ataque DoS semelhante lançado contra a Dyn, um grande provedor de serviços de Internet.[227]

---

[227] Para o assunto, vide BUTLER, Alan. *Products liability and the internet of (insecure) things:* Should Manufacturers Be Liable for Damage Caused by Hacked Devices?, 50 U. Mich. J. L. Reform 913, p. 913-915, 2017. Disponível em <http://repository.law.umich.edu/mjlr/vol50/iss4/3>. Acesso em: 2 maio 2018. Veja, também no Centro de Estudos, Respostas e Tratamento de incidentes de segurança no Brasil – CERT.BR. *Cartilha de segurança para internet*. A Negação de serviço, ou DoS (Denial of Service), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (Distributed Denial of Service). O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo. Quando isto ocorre, todas as pessoas que dependem dos recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas. Nos casos já registrados de ataques, os alvos ficaram impedidos de oferecer serviços durante o período em que eles ocorreram, mas, ao final, voltaram a operar normalmente, sem que tivesse havido vazamento de informações ou comprometimento de sistemas ou computadores. Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques. A grande maioria dos computadores, porém, participa dos ataques sem o conhecimento de seu dono, por estar infectado e fazendo parte de botnets. Disponível em: <https://cartilha.cert.br/ataques/>. Acesso em: 26 abr. 2018.

O custo médio de um ataque cibernético de negação de serviço ("DoS") pode chegar a US $ 1,5 milhão e no pico do ataque a Dyn, a rede de dispositivos hackeados estava enviando estimados 1,2Tbps de tráfego para os servidores da empresa.[228] Após um ataque de negação de serviço, o suporte técnico e custos de ativos danificados podem ser mais do que US $ 100.000 e esse valor não inclui a receita perdida devido ao tempo de inatividade ou outras interrupções nos negócios. O ataque ao site de Krebs é dado como exemplo de que os dispositivos conectados, as coisas, cada vez mais são alvo de hackers e utilizados para realizar ataques cibernéticos caros e devastadores.

Há estudos que indicam que softwares maliciosos e com possibilidade de aproveitar da arquitetura da IdC/IoT já foram desenvolvidos e no futuro os ataques podem ter origem em casas e veículos automatizados, o que de fato já ocorreu, pois o site de Krebs foi atacado com a ajuda de um *botnet* que escravizou um grande número de dispositivos, tais como roteadores, câmaras e gravadores de vídeo digital (DVRs).[229] Ao que parece, há a franca possibilidade de os ataques repousar na vulnerabilidade de senhas e dos próprios softwares, os quais não são atualizados remotamente por falta de diligência do fabricante ou esses equipamentos são fabricados com baixos padrões de segurança.

Dados os enormes custos incorridos pelas vítimas de DoS e outros ataques de rede, o papel central que os dispositivos conectados desempenham nessas ataques, e o

---

[228] Para os dados citados, confira-se as citações colhidas em BUTLER, Alan. *Products liability and the internet of (insecure) things*: should manufacturers be liable for damage caused by hacked devices?, 50 U. Mich. J. L. Reform 913, p. 913-915, 2017. Disponível em: <http://repository.law.umich.edu/mjlr/vol50/iss4/3>. Acesso em: 18 abr. 2018.

[229] Ibidem, *apud* TECHS, Akamai. Q2 2016 Report, 3 ST. OF THE INTERNET / SECURITY, no. 2, 2016, at 40, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2- 2016-state-of-the-internet-security-report.pdf>. "Bot" é um tipo de *malware* que permite ao hacker ou cracker obter controle completo através de uso remoto de um computador afetado. Ou seja, transforma um computador em um "zumbi" para realizar tarefas de forma automatizada na Internet, sem o conhecimento do usuário. Uma botnet, por sua vez, é uma rede de agentes de software ou *bots* que executam autonomamente. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/03/o-que-e-botnet.html >. Acesso em: 3 maio de 18.

grande número de potenciais vítimas espectadoras, provavelmente haverá um aumento constante nos litígios relacionados à IoT.[230]

Todos esses casos citados podem ser objeto de solução com base no que já dispõe o nosso ordenamento jurídico, notadamente para solucionar no campo da responsabilidade civil do fabricante e do fornecedor de serviços, o que se propõe oferecer algumas considerações adiante.

6. 5 Investigação criminal no rastreamento de "coisas" conectadas em rede.

Um crime ocorrido no dia 21 de maio de 2016, no Estado de Wisconsin nos Estados Unidos da América foi solucionado e provado mediante a análise de dados recolhidos por "coisas" conectadas à Internet. Segundo afirmado, o Big Brother estava assistindo como George Burch matou Nicole VanderHeyden.[231] Restou demonstrado que a pessoa de George Burch foi o assassino de Nicole VanderHeyden, pois a polícia conseguiu coloca-lo na cena do crime, mediante a análise dos dados do Google Dashboard, permitindo verificar que foi o responsável por abandonar o corpo da vítima em um local ermo, um campo da Hoffman Road, em Bellevue. Os detetives pegaram os dados do telefone celular do acusado e rastreá-lo, vendo os locais em que estivera na madrugada do assassinato, sendo que o autor do crime ao ser confrontado com as evidências tentou culpar uma outra pessoa.No entanto, a análise dos dados do relógio

[230] Para um resumo de variados casos nos últimos dez anos nos EUA, confira-se o estudo de FRAM, Robert D; FRANKEL, Simon J; LYNCH, Amand C. Standing in data breach cases: a review of recent trends. *Bloomberg BNA*, Nov. 9, 2015. Disponível em: <http://www.bna.com/standing-data-breach-n57982063308/>. Apud BUTLER, Alan. *Products liability and the internet of (insecure) things*: should manufacturers be liable for damage caused by hacked devices*?*, 50 U. Mich. J. L. Reform 913, p. 915, 2017. Disponível em: <http://repository.law.umich.edu/mjlr/vol50/iss4/3>. Acesso em: 20 abr. 2018.

[231] Esse caso foi amplamente noticiado nos Estados Unidos da América. *Vide*, SRUBAS, Paul. Burch claims fear of probation violation stopped him from reporting VanderHeyden murder. *USA Today Network-Wisconsin*. 28 fev. 2018. Disponível em: <https://www.greenbaypressgazette.com/story/news/2018/02/28/burch-scheduled-testify-his-own-defense-trial-murder-nicole-vanderheyden/380587002/>. Acesso em 3 abr. 2019.

Fitbit Flex, um dispositivo que colhe os dados de atividades físicas de uma pessoa, permitiu demonstrar que seria impossível a essa pessoa ter estado nos locais e horários do crime. Ainda, a polícia analisou o Snapshot, mecanismo instalado pela seguradora no carro da vítima, para descartar qualquer possibilidade de que o corpo de VanderHeyden poderia ter sido transportado em seu próprio carro.

O analista de crimes forenses Tyler Behling disse aos jurados que a Google usa torres de celulares, sinais de redes sem fio e informações de GPS para rastrear os locais e horários dos usuários de telefones, ou seja, o usuário não precisa ativar nada no seu telefone e as informações (dados) são colhidos em segundo plano, já que diferentes redes oferecem automaticamente seus serviços a telefones celulares que possam querer. A coleta desses dados permite concluir que tudo fica registrado. Há uma certa precisão do rastreamento, a depender do ponto exato em que o usuário (telefone) estiver, pois algumas torres ou sinais de Wi-fi são mais ou menos intensos. Naquele julgamento, um perito forense demonstrou aos jurados, com o apoio de um mapa dos locais, os locais em que o acusado Burch estivera.

Os dados extraídos do navegador do telefone de Burch, permitiram demonstrar que realizara dezenas de buscas por informações sobre a investigação do assassinato de Nicole VanderHeyden. No caso de Burch, os dados colhidos pela Google o colocara às 3h04 da manhã nas proximidades, seja na casa da vítima, na rua ou no quintal do vizinho, mas estivera mais ou menos ali. As redes Wi-fi, três minutos antes, registrarm Burch na mesma área, com uma margem de erro ainda inferior.

As coisas melhoraram muito quando Burch entrou na Hoffman Road com o corpo de VanderHeyden. Lá, os sinais foram fortes o suficiente para colocá-lo com uma margem de erro de 32,8 pés e no campo da fazenda em que o corpo foi desovado, o raio de sua localização o colocava em uma uma distância de 9,84 pés, às 3h58 da manhã.

Em resumo, se você possui um Fitbit, essa coisa sabe mais sobre suas atividades do que você mesmo. Importante mencionar que no caso do assassinato, a fase da execução do chamado Caso Marielle, a utilização da tecnologia e a análise dos dados

colhidos pelas operadoras de telefonia celular e de acesso à internet que permitiram a elucidação, culminando com a prisão dos executores materiais do crime.[232]

7. **Do vazio normativo à solução pelo ordenamento jurídico brasileiro**

Dos casos anteriormente referidos podemos extrair a necessidade de uma legislação específica para a nossa ordem jurídica e na aparente ausência de regramento próprio, extrair das normas legais existentes uma interpretação às questões que venham a ocorrer. Assim decorre, pois os usos da Internet estão cada vez mais amplos no Brasil, notadamente no campo da utilização das "coisas" conectadas na rede.

Quanto à coleta, tratamento de dados e anonimização, em breve entrará em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), a Lei nº 13.709/2018, legislação que regulará as atividades de tratamento de dados pessoais, com alterações nos artigos 7º e 16 do Marco Civil da Internet.[233]

Indubitavelmente, as diferentes ordens jurídicas já tratam em alguma partida da questão da necessidade da proteção dos dados pessoais, dada a vulnerabilidade na sua conservação e compartilhamento, de vazamentos desses dados, de usos indevidos, da anonimização dos dados e de suas falhas, permitindo a reversão (reidentificação) etc. As empresas coletoras e gestoras de dados podem desenvolver os melhores meios de proteção dos dados colhidos, mas é preciso disciplinar com regras claras os processos de coleta e de tratamento desses dados, do compartilhamento com ou sem a anonimização. O debate do espectro dessas situações já é uma realidade e deve

---

[232] FÁVERO, Bruno. Caso Marielle é exemplo de como tecnologia pode ajudar a solucionar crimes: policiais usaram dados de telefonia e de aplicativos para chegar aos acusados. *Folha de São Paulo*, 15 mar. 2019. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2019/03/caso-marielle-e-exemplo-de-como-tecnologia-pode-ajudar-a-solucionar-crimes.shtml>. Acesso em: 3 abr. 2019.

[233] Cabe referir que o período inicial de *vacatio legis* de 18 meses foi alterado para 24 meses, com a MP Nº 869/2018. O texto aprovado originalmente pelo Parlamento brasileiro previa a criação da Autoridade Nacional de Proteção de dados, vetado e recriado pela MP referida, tema que não será enfrentado, por ora, no escopo deste ensaio.

avançar nos Estados Unidos[234], até porque a União Europeia está com um notável avanço no meio, como é a Regulação Geral de Proteção de Dados da Comunidade Europeia (GDPR, na sigla em inglês), que entrou em vigor a partir de maio de 2018 e unifica a legislação dos países europeus sobre o tema.

Em contrapartida e diferente do modelo europeu, os Estados Unidos tratam da questão de proteção de dados em leis setoriais no âmbito federal, com algum tratamento nos estados da federação.[235] A propósito, a partir da década de 1960, o Governo dos EUA começou a informatizar os dados sobre seus cidadãos e combinando-os em massivos bancos de dados, causando enorme preocupação com a privacidade e em 1973, um comitê consultivo criado pelo Secretário da Saúde, Educação e Assistência Social emitiu um substancioso relatório sobre o tema, propondo uma estrutura nova chamada de "Fair Information Principles", os FIPS, exigindo um esquema de proteção aos dados, com aviso, consentimento, acesso, integridade de dados, aplicação e remédios (jurídicos).[236] Destaca Paul Ohm, influenciados pelos FIPS, os legisladores editaram leis destinadas a evitar os "privacy problems" que não têm nada a ver com o "injury to feelings" no cerne dos atos ilícitos de violação da privacidade.[237]

A nossa lei da proteção de dados sequer entrou em vigor, mas certamente causará um grande impacto nos negócios das empresas prestadoras de serviços, não somente na Internet, pois a lei vale para o mundo Online como o Offline. O regime legal a entrar em vigor prevê diversos mecanismos de proteção legal, no sentido de imputar responsabilidade civil, de maneira objetiva, ao recolhedor dos dados quando forem compartilhados de forma indevida, notadamente pelos vazamentos, da anonimização

---

[234] Para o assunto, vide em OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *Ucla Law Review*, v. 57, p. 1733-1734, 2010.

[235] *Vide* o ensaio de GUIDI, Guilherme Berti de Campos. *Modelos regulatórios para proteção de dados pessoais*. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 3 abr. 2019.

[236] OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *Ucla Law Review*, v. 57, p. 1733-1734, 2010.

[237] Ibidem, p. 1734.

e de eventuais falhas que permitam a sua reversão, seja por métodos legais ou ilegais.

No Brasil, há uma aparente falta de regulação específica para os procedimentos de coleta, compartilhamento e uso de dados dos consumidores. Mas há alguns delineamentos em diversas normas que não podem ser descurados e servem para apreciação dos casos concretos. Portanto, enquanto não entrar em vigor a legislação própria, devemos buscar no que já contamos de regramento para afirmar, de legislação adequada para frear os abusos rotineiros.

Deve ser levado em conta, antes de qualquer outra consideração, a Constituição Federal já dispõe sobre a proteção de dados e notadamente a questão do direito à intimidade e à vida privada, contornos que não são analisados na seara estrita deste ensaio. Não vamos tratar das escalas da privacidade, assunto que merece um tratamento mais aprofundado em um ensaio com esse enfoque. Por ora, a menção ao Código Civil, legislação que já cuida de dispor quanto à privacidade, pois o considera como um direito decorrente da personalidade.

O Dec. 52.026/1963, que regulamenta a Lei Geral das Telecomunicações, que não é o caso de internet, dispõe que dados são sinais especiais, portadores de informações destinadas à execução automática de controles ou estudos de diversas espécies, veiculados através de linhas ou circuitos de telecomunicações.

Mais precisamente quanto à coleta automática ou não de dados pelas "coisas", há três diplomas legais a ser usados de apoio na tarefa de resolver as intrincadas questões, em um esforço de construção sobre os limites e os deveres a serem cumpridos pelos prestadores de serviços e fornecedores de produtos com conexão em rede de internet. Assim, ao intérprete o cuidado de observar o regramento existente na lei do cadastro positivo e suas recentes alterações, a lei do marco civil da internet e o campo maior de incidência em nosso Código de Defesa do Consumidor.

A Lei nº 12.414/2011, lei do cadastro positivo, estabelece um conjunto de regramento a ser perfeitamente adaptável às circunstâncias específicas da coleta de dados, pois configura um marco mínimo de obediência no processo da recolha de dados.

PROGRAMA DE PÓS-GRADUAÇÃO MESTRADO PROFISSIONAL EM DIREITOS SOCIAIS E PROCESSOS REIVINDICATÓRIOS/PPGDIesb - ISSN: 2448-2358

O legislador proíbe as anotações dos considerados dados sensíveis, afirmando que tais são aqueles pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas. (art. 3°, § 3º , II,).

Ainda, a recolha de dados exige que as informações sejam objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado (Art. 3°, § 1°). O art. 4°, da Lei do cadastro positivo requeria a autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada. Essa realidade mudou, por exigências do mercado financeiro, sendo que a redação atual do artigo mencionado autoriza a coleta e abertura de cadastro em banco de dados, sem ônus ao cadastrado e com a obrigação legal de posterior comunicação ao consumidor, desde que já não tenha cadastro anterior, o que dispensaria essa comunicação.

A anterior redação do art. 9°, da Lei do Cadastro Positivo somente permitia o *compartilhamento* de informação quando autorizado expressamente pelo cadastrado, por meio de assinatura em instrumento específico ou em cláusula apartada, o que deixou de existir, pois a atual redação permite o compartilhamento da mesma forma que de sua recolha. Dessa forma, o legislador estatuiu uma inversão da inserção em cadastro de bancos de dados de créditos na forma positiva, cabendo ao consumidor a posteriori exercer o direito de cancelar uma inscrição.

Por seu turno, a Lei do Marco Civil da Internet – LMCI (Lei 12.965) dispõe de importantes anotações e de um modelo de regramento que cabem como uma luva a vários dos casos abordados anteriormente, notadamente às questões das TVs "smart" e do brinquedo sexual, senão vejamos:

O fato de as "coisas" utilizarem das funcionalidades da internet atrai a lei do marco civil da internet para enfrentamento e as aplicações de internet que as coisas oferecem desconsidera os direitos básicos dos consumidores consagrados além do CDC, notadamente quanto ao disposto na LMCI.

Para abertura, confira-se desde logo o dever de proteção estatuído aos prestadores de serviços em internet, na linha do que dispõe o artigo 10º da referida lei, regendo que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata a lei em causa, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

A LMCI veda o fornecimento a terceiros dos dados pessoais coletados, notadamente os registros de conexão e de acesso a aplicações de internet. Vejamos:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: VII - **não fornecimento a terceiros de seus dados pessoais**, inclusive registros de conexão, e de acesso a aplicações de internet, salvo **mediante consentimento livre, expresso e informado** ou nas hipóteses previstas em lei;

Naquelas situações dos casos de direito comparado, acaso o intérprete brasileiro fosse chamado a solucionar, a primeira pergunta a ser feita e de resolver, seria perquirir de justificativa razoável na coleta dos dados dos consumidores, além de investigar qual teria efetivamente o benefício que o consumidor pode obter com a coleta de seus dados, notadamente para obtenção da fruição da coisa conectada em rede.

A propósito, vejamos os incisos desse artigo que devem ser invocados:

> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

Não obstante a LMCI trate o consumidor como usuário, temos a exata compreensão de que neste feixe de dispositivos comercializados e com serviços de internet há a figura do consumidor, do fornecimento de um produto e de um serviço e

PROGRAMA DE PÓS-GRADUAÇÃO MESTRADO PROFISSIONAL EM DIREITOS SOCIAIS E PROCESSOS REIVINDICATÓRIOS/PPGDIesb - ISSN: 2448-2358

há remuneração direta e indireta. Em suma, temos todos os elementos de uma relação jurídica de consumo (art. 2° e 3° do CDC).

Encontrado a justificativa para aplicação do CDC, deve ser visto que nas sempre preciosas lições do diálogo das fontes referida por Cláudia Lima Marques[238], a LMCI cabe como uma luva para afirmar, desde logo, do aumento considerável dos direitos básicos dos consumidores, ao consagrar em seu art. 7º de outros direitos que são assegurados, dentre eles o de não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas demais hipóteses previstas em lei.

O Decreto regulamentador da LMCI trata em seu art. 13 sobre padrões de segurança a ser observado pelos fornecedores, notadamente na questão do uso de soluções de gestão para assegurar a inviolabilidade dos dados e ainda trata da exclusão da coleta dos dados, tão logo atingida a finalidade de seu uso.

Fosse o caso da TV VIZIO sob a égide da lei brasileira, dúvida nenhuma de ser uma relação jurídica de consumo e de que ocorrido teria a violação da LMCI. Da forma como relatado do agir da empresa, não teria ocorrido, por exemplo, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais, uma vez que esses somente podem ser utilizados para as finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. Como diz respeito a coleta de dados diretamente envolvidos com a privacidade do consumidor, em seu aspecto mais profundo, a permissão de coleta dos dados deve ser precedida de uma informação completa antes de sua coleta, a fim de permitir ao

[238] MARQUES, Cláudia Lima. *Diálogo das fontes*. In: BENJAMIN, Antonio Herman V., MARQUES, Claudia Lima, BESSA, Leonardo Roscoe. *Manual de direito do consumidor*. 8. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2017. p. 1145-162.

consumidor exercer o direito de escolha entre aderir ao serviço oferecido ou ou de recusá-lo.

Mais o que parece ser o mais grave, a conduta da empresa fabricante da TV VIZIO estaria com franco antagonismo ao direito assegurado de o dado somente ser coletado com o consentimento expresso sobre a coleta, do uso, do armazenamento e do eventual tratamento dos dados pessoais, eis que segundo a nossa legislação, deve ocorrer de forma destacada das demais cláusulas contratuais.

E ainda, a VIZIO não ofereceu os meios para ao consumidor a exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas na Lei do Marco Civil da Internet.

Como se vê, a lei existente em nosso ordenamento jurídico é suficiente para a miríade de casos vistos no horizonte da internet das coisas. Ademais, o Código de Defesa do Consumidor (Lei 8.078, art. 6º, III) é expresso no direito básico do consumidor em ter informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem.

E se há o direito básico do consumidor, há ainda o dever jurídico de prestar tais informações, necessárias e adequadas a seu respeito, pelo risco inerente (periculosidade). Ainda, há o dever da informação sobre os riscos que podem apresentar à saúde e segurança, conforme previsão do art. 31, do Código de Defesa do Consumidor.

O descumprimento do dever de informar é uma prática abusiva (art. 39 do CDC), eis que a abertura do texto, ao aludir que entre outras práticas, permite a linha da interpretação proposta e ainda podemos dizer que no campo da internet das coisas, a fabricante da TV VIZIO incidiu na previsão do inciso IV desse artigo 39, qual seja, a de prevalecer-se da ignorância do consumidor (vulnerabilidade informacional), notadamente quanto ao conhecimento da técnica de coleta de dados e não ter dado opção de recusa dessa coleta.

É possível que no campo da internet das coisas, a imensa maioria dos consumidores deve ser compreendida como hipervulneráveis ou com uma vulnerabilidade agravada, em razão da técnica empregada e dos possíveis riscos do que pode ser feito ou já o ocorre com os dados coletados.

Se para a coleta dos dados da TV VIZIO já há subsunção, com mais razão ainda às práticas da empresa fornecedora de brinquedos sexuais com ampla coleta dos hábitos de seus usuários. Os avisos que a empresa diz efetuar não parece ser suficiente para evitar qualquer imputação de responsabilidade civil, pois seguramente um grande contingente de adquirentes deixaria de comprá-lo, acaso soubesse de que seus hábitos são monitorados e colhidos.

No caso do brinquedo erótico, estamos diante de um produto/serviço com um grau maior do que o simples risco inerente, mas sim do que pode ser produzido com o tratamento dos dados em termos informacionais à privacidade no seu grau máximo, da própria intimidade de natureza sexual. É a típica hipótese dos produtos e serviços potencialmente nocivos ou perigosos à saúde ou segurança e que exigem, a prestação de uma informação de maneira ostensiva e adequada, a respeito da sua nocividade ou periculosidade (Art. 9°, do CDC).

Claro, há quem possa sustentar que o risco seja meramente o risco inerente, o que de qualquer modo passa pelas exigências de a autorização da coleta dos dados deva ser precedida de informações claras e adequadas e devem ser restritas às finalidades próprias da utilização do brinquedo.

Quanto aos veículos, dos riscos de automóveis e caminhões ser invadidos seus sistemas inteligentes por hackers ou crackers, é lição básica de direito do consumidor, de que o fornecedor de produtos e serviços no mercado de consumo deve atender aos critérios de qualidade segurança e que todo produto e serviço possui os riscos inerentes ou riscos exarcebados, em razão de serem potencialmente nocivos ou perigosos. Enquanto os riscos estiverem dentro desse patamar, até porque não há como eliminá-los totalmente, seja pelos custos altíssimos que tornariam tais produtos inviáveis no

mercado, notadamente pelos custos ou o produto perderia a sua utilidade, o certo é que as descobertas de falhas de segurança a posteriori de seu lançamento no mercado de consumo, impõe uma leitura um pouco diferenciada da solução das Cortes Americanas.

Com efeito, em sendo descobertas vulnerabilidades de segurança nos veículos espertos, com a probabilidade latente de ser invadida e de terríveis consequências, estamos frente a um produto ou serviço que apresenta um alto grau de nocividade ou periculosidade à saúde e segurança (art. 10º, do CDC) e gera o dever de recall, seja por atualizações dos mecanismos de segurança de forma remota, quando houver a possibilidade pelas funcionalidades, seja pelo chamamento dos consumidores, além da necessária campanha publicitária informativa (§ 1º do art. 10º do CDC).

No que tange a possibilidade de ser um produto enquadrado como defeituoso, deve ser lembrado o momento em que o produto foi colocado em circulação, circunstância para avaliar a presença de defeito.

Porém, na hipótese de vier a ser descobertas falhas na performance de segurança, posteriores ao seu lançamento no mercado, não estamos mais apenas presente no campo das expectativas, mas sim com riscos de o produto estar com um alto grau de nocividade ou periculosidade, o que exige de seu fabricante além da campanha de alerta, o desenvolvimento de mecanismos tecnológicos que corrijam as falhas ou até mesmo de exigir o seu recolhimento, para evitar a ocorrência de um acidente de consumo.

Decorrente da possibilidade ou da real ocorrência de ações maléficas por crackers, tanto no caso de veículos automatizados, como em uma linha imensa de "coisas", algumas ponderações são anotadas:

a) da segurança legitimamente esperada - é preciso ponderar se a invasão por hackers ou crackers, por si só, torna o produto ser defeituoso, pelo fato de não oferecer a segurança que dele legitimamente se espera.

Sem esgotar o assunto, há algumas variáveis a ser ponderadas.

Primeiro, a invasão por hackers foi possível em decorrência da escolha pelo fabricante do design de seu produto, dos mecanismos de segurança? O fabricante sabia ou deveria saber da falha de segurança à época do lançamento do produto no mercado, ao colocá-lo em circulação? A resposta positiva parece induzir de ser um defeito do produto, meramente um fortuito interno, pois decorrente da má escolha do fornecedor. Nesse caso, há defeito, palavra-chave que torna o fornecedor responsável pelos acidentes de consumo.

Não podemos esquecer, o caso de responsabilidade objetiva pela teoria do risco, ex vi do art. 927, parágrafo único, parte final, do Código Civil. Ou até o caso do art. 931, do CC. De qualquer sorte, a responsabilidade objetiva caminha pari passu na ocorrência de defeito do produto, pois não é o caso de uma previsão normativa própria do grau de responsabilidade e até mesmo nas hipóteses do art. 931 do CC há a necessidade da presença da palavra-chave defeito.

Segundo, embora previsível a invasão por hackers/crackers nas "coisas" o grau de segurança adotado por ocasião da colocação do produto no mercado era suficiente para frear as invasões, de acordo com os conhecimentos científicos da época? Se a resposta for sim, parece que não há o que se falar em defeito e não é risco do desenvolvimento.

Terceiro, as vulnerabilidades de *software* apresentam problemas sempre em evolução, pois os pesquisadores de segurança e os hackers estão constantemente descobrindo novas vulnerabilidades, e essas descobertas exigem dos fabricantes a atualização dos seus produtos.239 A atualização deve ser dada por um eficiente serviço pós venda, pois as empresas de software têm um maior grau de controle sobre o uso,

---

[239] BUTLER, Alan. *Products liability and the internet of (insecure) things*: should manufacturers be liable for damage caused by hacked devices?, 50 U. Mich. J. L. Reform 913, p. 928, 2017. Disponível em: <http://repository.law.umich.edu/mjlr/vol50/iss4/3>. Acesso em: 20 abr. 2018. Anotou Alan Butler, "Security researchers and hackers are constantly discovering new vulnerabilities, and these discoveries require software vendors to update their software on a regular basis.

monitoramento e manutenção de seus produtos, o que deve ser exigido dos fornecedores, ao imputar a responsabilidade de resolver pelos defeitos surgidos após a colocação no mercado de consumo. E mais ainda, há a exigência latente de dar os avisos necessários para correção das falhas de segurança que vierem a ser descobertas após a colocação do produto no mercado e em sendo um produto passível de ser corrigido à distância (remotamente), nada mais crível de que o fabricante tenha a capacidade de forçar o consumidor a atualizar seu produto, o que pode ser um meio eficiente para evitar acidentes de consumo.

Quarto, não há garantia de que o consumidor tomará os passos afirmativos para corrigir os bugs, o que pode tornar emblemática a imposição de responsabilidade meramente pelo campo dos acidentes de consumo naqueles casos em que o consumidor não atende às campanhas de recall.

Nesse caso, ou o fabricante adota as medidas para forçar a atualização e impeça o consumidor de usufruir de sua "coisa" enquanto não proceder na atualização de segurança ou se não o fizer, deverá responder o fornecedor pelos danos causados, e a solução repousa na imposição de responsabilidade, dentro do que se convenciona para as lições tradicionais dos acidentes de consumo causados nos produtos e serviços em que há campanhas de recall e o consumidor permaneceu inerte.

Logo, não há como eximir o fabricante pelos danos causados aos consumidores vítimas de acidente de consumo por produtos invadidos por hackers, nas hipóteses em que deixou de atualizar seus mecanismos de segurança, ao tomar conhecimento das vulnerabilidades. Acaso for concluído pela irresponsabilidade no caso de ataque de hackers, os fabricantes não teriam incentivos para aprimorá-los e realizar os necessários investimentos.

E em quinto e último lugar, as ações dos piratas da internet, os crackers, são excludentes do dever jurídico de indenizar? Pode ser considerada uma hipótese do fortuito externo? A literatura é farta da ocorrência de invasão de sistemas de segurança por ataques cibernéticos e não há nenhum mecanismo cem por cento seguro. O ataque

é previsível e por mais cautelas que o fabricante venha a adotar, sempre será possível apurar uma falha de segurança, pois é risco normal do meio. Adotadas pelo fabricante de todas as cautelas propostas, é razoável afirmar que a ultrapassagem dos mecanismos de segurança pode ensejar a aplicação da excludente por fato (culpa) exclusiva de terceiro, o que exigirá do juiz muita cautela para decidir e de munir das necessárias perícias.

No caso de Banco, é pacífico a incidência do dever de indenizar, de ser o caso da aplicação da responsabilidade objetiva, pois é um risco da atividade e não se pode imputar a ação de hacker, na clonagem de dados, de senhas ou outras atividades nocivas, como excludentes do dever jurídico da responsabilidade civil, muito embora algumas decisões isoladas afastam o dever dos agentes financeiros, notadamente considerando ser uma ação de terceiro, máxime quando há cópia da senha, eis que cabe ao consumidor conservá-la em local seguro.

O desenvolvimento de uma teoria consentânea com a internet das coisas ainda está em seus primórdios, exigindo maiores estudos, mas por ora são essas as primeiras anotações para os problemas suscitados.

Indubitavelmente a Internet faz parte da vida da humanidade e todos nós estamos conectados em rede. Os problemas jurígenos advindos da era da Internet não parecem ser muito diferentes dos que já ocorriam antes de sua ampla disseminação, notadamente na fase mais atual, a chamada Internet das coisas.

Ao jurista, o papel de investigar as especificidades do meio virtual e vislumbrar como resolver as questões, passando pela análise serena do sistema jurídico sem ferir o pleno desenvolvimento da rede de Internet e a capacidade de inovação.

Considerações finais

Não se pode aduzir desde logo em uma resposta direta e conclusiva para todas as questões, pois ainda o papel da doutrina e da jurisprudência poderá oferecer

respostas outras ao que foi proposto neste ensaio. No entanto, desde logo pode ser afirmado que o Código de Defesa do Consumidor desempenha papel fundamental para a solução dos litígios e os fornecedores de "coisas" conectadas em rede devem cumprir com os deveres de somente colocar no mercado produtos seguros, observando rigorosamente os deveres de fornecer informações plenas e adequadas aos consumidores, pois é direito básico o de receber tais informações, para escolhas conscientes a partir do momento em que há a ciência do risco envolvendo a fruição das novas tecnologias.

Referências

A SOCIEDADE da informação. *In:* TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil:** livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Capítulo 1. p. 5

AVANCINI, Helenara Braga. O paradoxo da sociedade da informação e os limites dos direitos autorais. In: ROVER, Aires José. (Org). **Direito e informática**. Barueri, SP: Manole, 2004.

BALLESTEROS MOFFA, Luis Ángel. **La privacidad electrónica***:* internet em el centro de protección. Valencia: Tirant L lanch: 2005.

BUTLER, Alan. **Products liability and the internet of (insecure) things**: should manufacturers be liable for damage caused by hacked devices?, 50 U. Mich. J. L. Reform 913, 2017. Disponível em: <http://repository.law.umich.edu/mjlr/vol50/iss4/3>. Acesso em: 18 abr. 2018.

CASTELLS, Manuel. **Internet e sociedade de rede:** lliçó inaugural del programa de doctorat sobre la societat de la informació i el coneixement. Disponível em: <http://www.uoc.edu/web/cat/articles/castells/print.html>. Acesso em: 30 abr. 2017.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.BR. **Cartilha de segurança para internet**. Disponível em: <https://cartilha.cert.br/ataques/>. Acesso em: 26 abr. 2018.

DRUMMOND, Victor. **Internet, privacidade e dados pessoais**. Rio de Janeiro: Lúmen Júris, 2003.

DUFF, Alistair S. **Information society studies**. Nova York: Psychology Press, 2000. v. 3.

FÁVERO, Bruno. Caso Marielle é exemplo de como tecnologia pode ajudar a solucionar crimes: Policiais usaram dados de telefonia e de aplicativos para chegar aos acusados. **Folha de São Paulo**, 15 mar. 2019. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2019/03/caso-marielle-e-exemplo-de-como-tecnologia-pode-ajudar-a-solucionar-crimes.shtml>. Acesso em 3 abr. 2019.

FIQUE atento, sua Smart TV pode estar espionando você e sua família. **IDGNOW**. Disponível em: <http://idgnow.com.br/ti-pessoal/2018/04/22/fique-atento-sua-smart-tv-pode-estar-espionando-voce-e-sua-familia/>. Acesso em: 9 maio 2018.

FRADA, Manuel A. Carneiro da. Vinho novo em odres velhos? A responsabilidade civil das "operadoras de internet" e a doutrina comum da imputação de danos. *In:* **DIREITO da sociedade da informação**. Coimbra: Ed. Coimbra, 2001. v. 2. p. 7-32.

FRAM, Robert D; FRANKEL, Simon J; LYNCH, Amand C. Standing in Data Breach Cases: **A Review of Recent Trends**, BLOOMBERG BNA, Nov. 9, 2015. Disponível em: <http://www.bna.com/standing-data-breach-n57982063308/>. Acesso em: 20 abr. 2018.

GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais.** Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 3 abr. 2019.

GORMAN, Leta E. The era of the internet of things: can product liability laws keep up? **Defense Counsel Journal,** v. 84, No. 3. Disponível em: <https://www.iadclaw.org/publications-news/defensecounseljournal/the-era-of-the-internet-of-things-can-product-liability-laws-keep-up/> Acesso em: 17 abril 2018.

KARVALIC, László Z. **Information society dimensions.** Szeged, JATEPress Kiadó, 2010.

LORENZETTI, Ricardo L. *Comércio eletrônico*. Notas de Cláudia Lima Marques. São Paulo: Revista dos Tribunais, 2004.

MARTINS, Guilherme Magalhães. O direito ao esquecimento na internet. In: _____. (Coord). **Direito privado e internet**. São Paulo: Atlas, 2014.

MACHLUPT, Fritz. 1962, apud PEKARI, Catrin. The information society and its policy agenda: towards a human rights-based approach. **Revue Québécoise de Droit International,** v. 18.1, p. 60, 2005. Disponível em: <https://www.sqdi.org/wp-content/uploads/18.1_-_pekari.pdf>. Acesso em: 29 abr. 2017.

MADAKAM, Somayya; RAMASWAMY, R; TRIPATHI, Siddharth. Internet of things (IoT): **A literature review**. *Journal of Computer and Communications*, n. 3, p. 164-173, May 2015. (SciRes). Disponível em: <http://www.scirp.org/journal/jcc http://dx.doi.org/10.4236/jcc.2015.35021>Acesso em: 17 abril 2018.

MARQUES, Cláudia Lima. Diálogo das fontes. In: BENJAMIN, Antonio Herman V., MARQUES, Claudia Lima, BESSA, Leonardo Roscoe. **Manual de direito do consumidor.** 8. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2017. p. 1145-162.

MORO ALMARAZ, Maria Jesús. Servicios de la sociedad de la información y sujetos intervenientes. *In:* APARICIO VAQUERO, Juan Pablo e BATUECAS CALETRÍO, Alfredo. (Coord.) **Autores, consumidores y comercio electrónico**. Madrid: Colex, 2004. p. 108.

O'BRIEN, Michael H. **The internet of things**: the inevitable collision with product liability. Disponível em: <https://www.productliabilityadvocate.com/2015/02/the-internet-of-things-the-inevitable-collision-with-product-liability/>. Acesso em: 17 abr. 2018. Postado em 2 de fevereiro de 2015.

OHM, Paul. **The Rise and Fall of ISP Surveillance**. *U. ILL. L. REV.*, p. 1417, 2009.

OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, v. 57, p. 1701-1777, 2010.

OLIVEIRA ASCENSÃO, José. **Estudos sobre direito da internet e da sociedade da informação**. Coimbra: Almedina, 2001.

PAESANI, **Direito e internet**: Liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2003.

PAVÃO, Samantha. **Tudo o que você precisa saber sobre engenharia social.** Postado em 26 janeiro de 2018. Disponível em: <https://www.psafe.com/blog/o-que-e-engenharia-social/> . Acesso em: 9 maio 2018.

PEKARI, Catrin. The Information Society and its policy agenda: Towards a human rights-based approach. **Revue Québécoise de Droit International**, v. 18.1, 2005. Disponível em: <https://www.sqdi.org/wp-content/uploads/18.1_-_pekari.pdf>. Acesso em: 29 abr. 2017.

RODRIGUES, Leonardo. Como se mede a audiência da TV aberta. **Tech Tudo**. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/07/como-se-mede-a-audiencia-da-tv-aberta.html >. Acesso em: 2 maio 2018.

SIQUEIRA JR., Paulo Hamilton Siqueira. Direitos Humanos e cidadania digital. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). **Direito & internet III:** marco civil da internet. São Paulo: Quartier Latin, 2015. t. 1. p. 176.

SIMÃO FILHO, Adalberto. Sociedade da informação e seu lineamento jurídico. In: PAESANI, Liliana Minardi (coord). **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

SRUBAS, Paul. Burch claims fear of probation violation stopped him from reporting VanderHeyden murder. **USA Today Network-Wisconsin**. Publicado em 28 fev. 2018. Disponível em: <https://www.greenbaypressgazette.com/story/news/2018/02/28/burch-scheduled-testify-his-own-defense-trial-murder-nicole-vanderheyden/380587002/>. Acesso em: 3 abr. 2019.

TOFFLER, Alvin. **Terceira onda**. Disponível em: <http://www.projeto.unisinos.br/humanismo/antropos/Terceira_Onda.pdf>. Acesso em: 19 ago. 2017.

TOFFLER, Alvin. **A terceira onda.** Rio de Janeiro: Record, 1980.

VICENTE, Dario Moura. **Direito internacional privado***:* problemática internacional da sociedade da informação. Coimbra: Almedina, 2005.

ICP. ANACOM. **O papel das comunicações no desenvolvimento da sociedade da informação:** relatório de regulação. p. 102. Disponível em: <http://www.anacom.pt/txt/template12. jsp?categoryId=85190>. Acesso em: 30 abr. 2017.

Reno v. **American Civil Liberties Union**. 521 U.S. 844 (1997).

SAMSUNG adverte: **Cuidado com o que você diz em frente a sua TV inteligente**. *O Globo,* 9 maio 2015. Disponível em <https://oglobo.globo.com/sociedade/tecnologia/samsung-adverte-cuidado-com-que-voce-diz-em-frente-sua-tv-inteligente-15286181>. Acesso em 17 abril 2018.

S.D. v. Hytto Ltd., d/b/a/ **Lovense Plaintiff**: S.D. Defendant: Hytto Ltd., d/b/a/ Lovense Case Number: 3:2018cv00688; Filed: January 31, 2018 Court: California Northern District Court Office: Oakland Office County: San Francisco Presiding Judge: Jeffrey S. White Nature of Suit: Other Statutory Actions Cause of Action: 28:1331 Jury Demanded By: Plaintiff. Disponível em: <https://www.courthousenews.com/wp-content/uploads/2018/01/Lovense.pdf> . Acesso em: 25 abr. 2018.

TECHS, Akamai. **Q2 2016 Report**, 3 ST. OF THE INTERNET / SECURITY, no. 2, 2016, at 40. Disponível em: <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2- 2016-state-of-the-internet-security-report.pdf>. Acesso em: 25 abr. 2018.