ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

A INTERNET DAS COISAS: UTILIDADES E RISCOS EM FACE AO DIREITO À PRIVACIDADE DOS USUÁRIOS

THE INTERNET OF THINGS: UTILITIES AND RISKS IN FACE OF USERS' RIGHT TO PRIVACY

RVD

Recebido em 15.08.2023
Aprovado em. 18.10.2023

Valéria Ribas do Nascimento[1]

Humberto Goulart Neto[2]

RESUMO
A velocidade com que os avanços tecnológicos ocorrem na sociedade em rede trazem mudanças nas formas de interação do indivíduo com o meio, havendo assim a necessidade de adequação a essas novas formas de interação. O direito à privacidade destaca-se como direito fundamental de primeira dimensão, sendo que sua construção se deu ao longo da história. No entanto, os avanços e inovações trazidas pelos dispositivos da Internet das Coisas, fazem com que haja uma mitigação do direito à privacidade, seja ela de forma voluntária por parte do indivíduo, ou mesmo de forma involuntária. Sendo assim, se faz importante o estudo do presente trabalho acerca das facilidades e inovações surgidas, não se desconsiderando os riscos inerentes ao seu uso frente ao direito à privacidade. Utiliza-se uma abordagem de forma dedutiva, sendo as técnicas de pesquisa utilizadas a bibliográfica e a documental.

PALAVRAS-CHAVE: Direito à privacidade; Direitos fundamentais; Internet das Coisas.

ABSTRACT
The speed with which technological advances occur in the network society bring changes in the forms of interaction of the individual with the environment, thus having the need to adapt to these new forms of interaction. The right to privacy stands out as a fundamental right of the first dimension, and its construction took place throughout history. However, the advances and innovations brought by the Internet of Things devices mean that there is a mitigation of the right to privacy, whether voluntarily on the part of the individual, or even involuntarily. Therefore, it is important to study the present work about the facilities and innovations that emerged, not disregarding the inherent risks of its use in the face of the right to privacy. A deductive approach is used, and the research techniques used are bibliographic and documental.

[1] Pós-doutora pela PUCRS; Doutora em Direito Público pela UNISINOS, com período de pesquisa na *Universidad de Sevilla* (US); Mestre em Direito Público pela UNISC; Graduada em Direito pela UFSM. Professora do Programa de Pós-Graduação em Direito da UFSM. E-mail: valribas@gmail.com ORDCID: 0000-0002-8602-8148

[2] Mestrando junto ao Programa de Pós-Graduação em Direito da UFSM. Graduado em Ciências Jurídicas e Sociais pela PUCRS. Bacharel em Gestão Pública pela UNINTER e em Ciências Militares – Área Defesa Social pela BMRS. E-mail: hgoulartneto@gmail.com ORCID: 0000-0003-0779-7465.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

KEYWORDS: Fundamental rights; Right to privacy; Internet of Things.

1 INTRODUÇÃO

A velocidade com que os avanços tecnológicos tem se desvelado na sociedade moderna faz com que esta própria tenha de se adaptar e se moldar às novas formas de inter-relações. Enquanto o direito à privacidade se afigura como direito fundamental com origem iluminista e construído ao longo de uma historicidade dos direitos fundamentais, a utilização de novas ferramentas faz com que o mesmo seja mitigado.

A utilização de diversos itens e produtos relacionados à internet das coisas, os quais permitem o acesso por parte dos sistemas de inúmeros dados dos indivíduos, gera uma atenuação ao direito à privacidade, ainda que de certa forma voluntária.

Dessa forma, o estudo do direito à privacidade no âmbito da sociedade da informação, e frente à utilização de dispositivos relacionados à internet das coisas, mostra-se de grande relevância. Isto porque um incontável número dos novos dispositivos e equipamentos de hoje são capazes de intercomunicação com a rede mundial de computadores, transmissão e recepção de dados dos seus usuários.

No presente estudo, utiliza-se uma abordagem de forma dedutiva, pois a pesquisa parte de uma situação ampla, cuja análise perpassa pelo direito à privacidade em um contexto histórico e na sociedade em rede, assim como pela internet das coisas (*Internet of Things – IoT*). Após, encaminha-se para a verificação de uma questão específica, acerca da mitigação do direito à privacidade no contexto da internet das coisas. As técnicas de pesquisa utilizadas caracterizam-se como bibliográfica e documental, pois são utilizados estudos de doutrinadores e documentos relacionados ao direito à privacidade e à internet das coisas.

Do método aplicado resultou a divisão do artigo em duas partes, sendo na primeira realizada uma contextualização histórica e considerações gerais sobre o direito à privacidade, enquanto no segundo capítulo, são abordadas as características e inter-relações da Internet das Coisas.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

A pertinência do estudo em questão se mostra relevante, haja vista que o crescente número de equipamentos e dispositivos utilizados no dia-a-dia são interligados à rede mundial de computadores, capazes de monitorar e transmitir dados dos usuários, devendo estes estarem atentos ao potencial malferimento ao direito à privacidade.

2 CONSIDERAÇÕES SOBRE O DIREITO À PRIVACIDADE NA ATUALIDADE

O direito à privacidade é direito fundamental consagrado constitucionalmente no âmbito do ordenamento jurídico brasileiro, estando previsto no artigo 5º, inciso X, da Constituição da República Federativa do Brasil (BRASIL, 1988) o qual dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

O reconhecimento de tal direito confunde-se com a própria história e afirmação dos direitos humanos, isto porque encontram suas raízes na teoria iluminista dos séculos XVII e XVIII, com esteio primordial na concepção de liberdades do indivíduo, garantindo-se que estes não sofressem interferências diretas do Estado, fatos estes que inclusive foram marcas das posteriores constituições escritas (Sarlet, 2012, p. 46). Neste esteio, sua classificação de direito fundamental relaciona-se aos direitos de primeira dimensão, ou seja, aqueles direitos de eficácia negativa, exigindo-se assim uma abstenção estatal em relação aos direitos exercidos pelos cidadãos (Silva, 2015).

Mais recentemente, pode-se citar a positivação e o reconhecimento do direito à privacidade na Declaração Universal dos Direitos Humanos, editada em 10 de dezembro de 1948, logo após o término da 2ª Guerra Mundial. Em seu artigo 12, o referido diploma legal preconiza "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei" (ONU, 1948).

Em igual linha, o Pacto Internacional sobre Direitos Civis e Políticos, de 1966, também previu o direito à privacidade como um postulado fundamental para a proteção

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

dos direitos dos cidadãos, na medida em que seu art. 17 (ONU, 1966) definiu que "Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação."

Nesse mote, observa-se a relevância que o direito à privacidade assume no contexto social, sendo amplamente reconhecimento nos mais diversos documentos legais nacionais e internacionais, sejam contemporâneos ou históricos. Todavia, diante dos crescentes avanços tecnológicos existentes, há de se perquirir até que ponto tais direitos se encontram efetivamente resguardados, em especial diante do advento cada vez mais pulsante e, por vezes inclusive de forma imperceptível para o usuário, de equipamentos relacionados à internet das coisas.

Com maior robustez a partir da década de sessenta do século passado, a sociedade passou por diversas mudanças, sendo caracterizada por Zygmunt Bauman como a sociedade da modernidade líquida. Nesta concepção, o sociólogo e filósofo polonês defende que as relações sociais e interpessoais estão relegadas a um segundo plano pela sociedade, haja vista que tais são fluídas e efêmeras, e também essa nova sociedade passa a objetivar com maior densidade a corrida pela aquisição de bens de consumo e produtos como forma de uma promessa de felicidade (Bauman, 2010).

Entrementes, o direito à privacidade na era da sociedade em rede tem sofrido consideravelmente com o advento das tecnologias ligadas à informática, as quais são capazes de coletar e processar um infindável número de informações dos usuários a cada clique. Dessa forma, "é lamentável, pois, reconhecer que o direito à privacidade tende a transformar-se, na atual era da informática, em piedosa ficção, caso não se logre criar uma instituição internacional capaz de se sobrepor a essa novíssima forma de imperialismo." (Comparato, 2003).

A superveniência de novas relações ligadas à informática em decorrência dos avanços tecnológicos faz com que seja necessária uma verificação mais amiúde dos direitos à privacidade frente a estas novidades.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

> O desenvolvimento da informática colocou em crise o conceito de privacidade, e, a partir dos anos 80, passamos a ter um novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações mesmo quando disponíveis em banco de dados.(Paesani, 2014)

O argumento da crítica de Fabio Konder Comparato em relação ao malferimento ao direito à privacidade, no caso citado, funda-se em relação às interferências ilegais não apenas do Poder Público, mas também de particulares, no tocante a escutas clandestinas em ligações telefônicas. Refere que apenas no final do século XX, estima-se que os Estados Unidos da América monitoravam cerca de quatrocentos milhões de ligações telefônicas por ano, sendo tais escutas, basicamente, mantidas e processadas pela sua Agência de Segurança Nacional (*National Security Agency* – NSA) (Comparato, 2003).

Assim, a tutela da privacidade torna-se um tanto mais maleável diante do próprio imbricamento da sociedade às características da sociedade da informação.

> Essa transitoriedade da privacidade é própria do dinamismo da vida social e do fato de que, no contexto da vida privada, desenvolvem-se operações de amplo espectro. Conforme oscile num ou noutro sentido, a vida é mais ou menos privada e, deste modo, mais ou menos protegida, quer em extensão, quer em profundidade. Obviamente, a tutela constitucional da privacidade é a mesma – defere uma garantia de inviolabilidade. Entretanto, conforme o atuar do privado existe maior ou menor amplitude de manifestação desta tutela. Naturalmente, é mais fácil verificar a infração ao preceito constitucional nas hipóteses em que o comportamento violador se dirija a aspectos mais próximos da intimidade do que postular sua verificação a aqueles que tangenciam a dimensão da vida pública. (Zanon, 2013)

Por certo que os avanços tecnológicos e dos meios de comunicação geram grande facilidades e comodidades para a sociedade moderna, sendo inconcebível a vida hoje sem muitos desses avanços que estão imbricados intimamente com o nosso modo de vida. No caso, não há como hoje se falar em sociedade e seus meios de interação, sem se falar em internet, celulares, computadores, dentre outros tantos meios.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

3 A INTERNET DAS COISAS E SUAS NUANCES FRENTE AO DIREITO À PRIVACIDADE

3.1. A evolução da internet

A Internet das Coisas se relaciona a uma nova era da comunicação e da internet, na qual, basicamente, pode-se interligar o mundo físico ao mundo virtual, por meios de dispositivos e aparelhos específicos de coleta de dados. Assim, para uma melhor compreensão dessa evolução, é necessária uma breve contextualização da evolução da internet e de seus meios de comunicação, até a fase na qual nos inserimos hoje.

A origem da internet remonta ao final da década de sessenta do século XX, na qual houve a criação por parte do Governo dos Estados Unidos da América do projeto *Advanced Research Projects Agency etwork* (Arpanet), com vinculação ao *Defense Advanced Research Projects Agency* (Darpa), sendo este um projeto bélico que serviu para a interconexão de redes militares (Castells, 2005).

A partir de então, seu desenvolvimento desbordou os limites dos aquartelamentos, sendo realizados convênios com universidades para fins do desenvolvimento dos protocolos de comunicações de dados entre redes de computadores sem a necessidade de existência de centros de controle entre as mesmas. Assim, a primeira rede de comunicação entrou em funcionamento em 1969, contanto com apenas quatro pontos de acesso, localizados na Universidade da Califórnia em Los Angeles, no *Standford Research Institute*, na Universidade da Califórnia em Santa Bárbara e na Universidade de Utah (Magrani, 2018).

Esta fase inicial da internet é conhecida como *web 1.0*, ou “web do conhecimento”, a qual era caracterizada pela interconexão entre as pessoas, ainda que de forma estática, sem que houvesse uma interatividade com o conteúdo disponibilizado na rede mundial de computadores. Dessa forma, também ficou conhecida pela denominação *read-only web,* sendo um exemplo bastante elucidativo da forma como funcionava essa interação eram os sites de compras. A aquisição de

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

produtos se dava pela escolha dos mesmos diante de catálogos virtuais disponibilizados de forma *online*, não sendo possível, no entanto, a interação com o *site* para apontamento de quantidades, cores, ou mesmo a aquisição online (Magrani, 2018, p. 65).

A transformação da internet com o passar do tempo se deu de forma gradual, sendo que embora não se possa apontar um marco temporal específico para a passagem da mesma para a era da *web 2.0*, este termo foi popularizado por membros da *O´Reily Media* em uma conferência realizada no ano de 2004. Esta segunda fase da web (*read-write web*) restou conhecida como "web da comunicação", pois a partir da mesma os usuários deixaram de ser apenas receptores do conteúdo produzido, mas passaram também à condição de protagonistas na produção do conteúdo (Magrani, 2018, p. 65).

Esse impulsionamento da condição dos usuários se deu tanto pela evolução das redes sociais, que permitiram a interação entre os mesmos, quanto pela criação de novas ferramentas de codificação de programas, que oportunizaram grandes mudanças no *e-commerce.* Neste caso, os *sites* de compras passaram a desenvolver uma interação com o usuário, seja por meio da possibilidade de aquisição dos produtos diretamente nos sites (inclusive com escolha de características específicas com relação a cor, numeração, modelo, *design*, etc), quanto à própria interação dos usuários com comentários, experiências de compras com outros clientes, dentre outras tantas ferramentas que são criadas (como gráficos de desempenho de produtos, indicações de produtos relacionados, etc) (Magrani, 2018, p. 66).

De igual sorte, também não há uma definição temporal de quando surgiu a *internet* 3.0, contudo a primeira aparição deste termo se deu 2006 pelo jornalista John Markoff, em seu artigo *Entrepreneurs see a web guided by commom sense,* publicado no *New York Times.* Também se destaca que este conceito, por ser ainda novo, é fluído e se encontra em construção, sendo possível o apontamento de pelo menos algumas características básicas.

Uma dessas características é o surgimento da *internet* semântica. Segundo Tim Berners-Lee, criador da *world wide web*, a *internet* semântica é integrante da *web* 3.0,

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

isto porque nas anteriores fases da internet o conteúdo era gerado para a compreensão humana, no entanto, nesta fase, o conteúdo também é destinado às próprias máquinas. Isto quer dizer que os dispositivos desta geração são capazes de obter, monitorar e interpretar informações e dados fornecidos ou captados dos usuários da rede. Assim, a *internet* 3.0 pode gerar resultados diferentes para as mesmas pesquisas, por exemplo, a depender do perfil do usuário que a está utilizando com base em seu histórico de navegação, local de acesso, dados climáticos do dia, etc (Magrani, 2018, p. 70-71).

Outra característica marcante desta fase é o fato de que os objetos podem interagir com os usuários, na medida em que são dotados de dispositivos e equipamentos capazes de interligar o mundo físico ao mundo virtual, sendo este o principal foco da *Internet* das Coisas.

3.2. A Internet das Coisas

A Internet das Coisas, também conhecida pelo acrônimo IoT, em decorrência de sua nomenclatura na língua inglesa (*Internet of Things*), encontra-se inserida intimamente na fase da *internet* 3.0. Nessa mesma linha das conceituações das fases da *internet*, o termo IoT não possui uma denominação estanque e única, mas pode-se utilizar como base a classificação elencada pelo professor Eduardo Magrani:

> A expressão IoT é utilizada para designar a conectividade e interação entre vários tipos de objetos do dia a dia, sensíveis à internet. Fazem parte desse conceito os dispositivos de nosso cotidiano que são equipados com "sensores capazes de captar aspectos do mundo real, como por exemplo temperatura, umidade e presença, e enviá-los a centrais que recebem estas informações e as utilizam de forma inteligente. A sigla refere-se a um mundo onde objetos e pessoas assim como dados e ambientes virtuais, interagem uns com os outros no espaço e no tempo (Magrani, 2018).

Assim, a Internet das Coisas inter-relaciona o mundo físico ao mundo virtual, e vice-versa. O conhecimento do mundo físico se dá diante da grande quantidade de dados minerados pelos sensores constantes desses dispositivos, sendo possível a

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

descoberta de comportamentos, tendências e, inclusive, a realização de interferências no tocante aos mesmos (Santos, et al, 2016).

Entrementes, não basta revestir qualquer objeto com um dispositivo capaz de comunicar-se com a rede mundial de computadores para que o mesmo possa ter uma aplicabilidade no espectro da *internet* das coisas. Inclusive já surge uma categorização chamada de *Internet das Coisas inúteis,* consistentes naqueles dispositivos em que a adaptação tecnológica não os aperfeiçoa ou trás benefícios para a sua utilização. Nestes casos, inclusive, entende-se que o objeto analógico é mais útil ao usuário do que aqueles com a tecnologia avançada envolvida, pois tendem a custar menos e terem uma utilização mais facilitada (Magrani, 2018, p. 47).

A lista de dispositivos desprovidos de uma aplicabilidade utilitária a amparar seu aperfeiçoamento ou benefícios de seu uso com base nos dispositivos tecnológicos, é grande. Um dos mais famosos é o *Egg Minder,* uma bandeja de ovos conectada a um aplicativo de celular que avisa quantos ovos estão na bandeja. Outro dispositivo conectado é o copo inteligente, capaz de identificar qual a bebida que há dentro do mesmo. O *RollScout* também é um desses produtos, tratando-se de um suporte para papel higiênico conectado ao *smartphone*, e que avisa quando o papel higiênico do rolo está chegando ao fim (Cardoso, 2018).

De outro lado, a lista de dispositivos ditos como úteis relacionados à Internet das Coisas é bastante ampla, havendo inclusive classificações quanto às suas utilidades. A classificação com maior amplitude e aceitação sobre o tema, subdivide os equipamentos de IoT em cinco campos: Saúde, físico e mental; bem-estar; segurança pessoal; e, privacidade de dados.

Importante categoria também é a do *wereables*, consistentes naquelas peças de vestuário que possuem conectividade com a Internet das Coisas. Essas tecnologias "vestíveis", permitem que os dispositivos aos quais as peças estão ligadas possam realizar leituras de informações produzidas pelo próprio usuário (sejam elas de forma voluntária ou mesmo de forma involuntária).

E são nesses pontos em que sobejam tantas facilidades e comodidades oferecidas por estas tecnologias, que também residem os perigos inerentes ao

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

malferimento aos direitos da privacidade dos usuários. Alguns dos dispositivos mais populares de IoT que podem ser elencados, são os *smartwatches* (relógios inteligentes), *smartbracelets* (braceletes inteligentes), dentre outros.

Tais produtos facilitam em muito a vida das pessoas, sendo possível o monitoramento de batimentos cardíacos tanto em repouso quanto em atividade física, a verificação da intensidade de alguns exercícios (seja por meio da velocidade de uma corrida a pé ou de bicicleta, ou mesmo o *pace* empregado), o itinerário que esse exercício é realizado, dentre inúmeras outras aplicações possíveis existentes e as que ainda serão inventadas.

As comodidades inerentes às tecnologias dispostas nos dias de hoje não param de surgir e não se exaurem nos exemplos acima. Também pode se exemplificar as diversas buscas realizadas em sites por meio dos celulares e a navegação veicular em aplicativos, no mais das vezes a interligação entre esses serviços é uma mola propulsora para anúncios e indicações para os usuários, como forma de direcionar sua vontade para determinada norte, conforme o interesse do patrocinador e anunciante dos serviços.

O crescimento vertiginoso da capacidade de captação de dados dos usuários por todos os meios possíveis, gera o desafio na segurança de dados no cenário da IoT, tendo em vista a necessidade de maior enfoque na gestão de armazenamento, servidores e redes de *data center*, assim como a maior responsabilidade de todos os operadores dessa rede de dados (Magrani, 2018, p. 92). Esse aumento do volume de dados em tráfego, aliado a transferência de dados entre os mais diversos serviços (dados captados por meio do itinerário feito por um corredor com um *smartwatch* podem servir para subsidiar anúncios de empresas na área em que essa pessoa corre), faz com que os riscos à privacidade sejam potencializados.

Mas não fosse apenas isso, há de se pontuar também a dificuldade dos usuários em ter o conhecimento do destino e da finalidade com que seus dados são colhidos, seja por falta de leitura dos termos do serviço, ou pela própria ausência de tais informações.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

Em primeiro, os usuários não possuem como costume a leitura dos termos de serviço, tanto pelo fato da dificuldade de compreensão de determinados documentos, quanto pela pressa na utilização dos serviços. Sobre este o ponto, inclusive algumas empresas de *software* já utilizaram desses contratos como forma brincadeira e para chamar a atenção da falta de leitura por parte dos usuários.

A empresa PC Pitstop, no ano de 2005, colocou nas cláusulas de seu contrato um prêmio de mil dólares, sendo que somente foi reivindicado tal premiação após cinco meses de lançamento do documento, e mais de três mil usuários cadastrados (ROMERO, 2017). Semelhante experimento foi realizado empresa GameStation, a qual colocou em seu contrato uma cláusula ao usuário de cessão da própria alma à empresa, sendo que mil pessoas identificaram a brincadeira, mas mais de sete mil aderiram aos termos de forma integral e irrestrita (Romero, 2017).

Tais situações vêm a corroborar pesquisa realizada pela Universidade de Stanford, na qual apontou que 97% dos usuários de serviços eletrônicos pulam direto para o concordo, e abrem mão de realizar a leitura dos termos de contrato e serviços das ferramentas que utilizam (Romero, 2017).

De mais a mais, outro ponto a se destacar acerca da coleta de dados, é a ausência de clara ciência acerca do destino dos dados coletados. Isto porque nem sempre o usuário possui a exata compreensão da extensão do alcance da utilização de seus dados. A fim de exemplificar, é possível elencar um aplicativo de monitoramento de corrida, sendo que o usuário não sabe se os dados monitorados (*pace* e itinerário) serão utilizados apenas para sua verificação do ritmo de corrida, ou se o algoritmo irá apresentar propagandas oportunamente de um tênis novo, de lojas ao redor do local de treino, etc.

Dessa forma, essa avidez com que as empresas possuem pela coleta de dados das mais diversas formas, impulsiona, nas palavras de Manuel Castells a “economia informacional, global e em rede.” (2005, p. 119). E ao analisar tais aspectos, Tatiana Malta Vieira (2007, p. 213) refere que essas características podem assim serem descritas, pois é informacional haja vista que a produtividade e a competitividade dependem da capacidade de produção, processamento e aplicação das informações e

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

dos conhecimentos gerados. É global, pois estas atividades e coletas de dados e informações se dão em escala mundial. E é em rede, pois essa economia se conecta das mais diversas formas. Mas e ainda que assim não fosse, também há de se gizar que uma proporção significativa dos próprios usuários dos meios tecnológicos fornecem de forma voluntária suas informações privadas e pessoais nas redes sociais (Véliz, 2021, p. 84).

Outro risco ao direito à privacidade dos usuários é a própria possibilidade de hackeamento dos dispositivos e utilização dos dados ali coletados (ou a serem coletados) com utilização de fim diverso ao almejado. O *boom* da utilização de dispositivos inteligentes fez com que esse mercado passasse a ser alvo de inúmeras empresas, tanto do ramo da tecnologia, quanto de outros ramos.

E embora esse alavancamento do mercado traga inúmeros benefícios, há pontos negativos a serem analisados. A agregação de dispositivos inteligentes em diversos produtos, sobretudo por empresas que não possuem um histórico na área de tecnologia e que buscam novos mercados e possibilidades para seus produtos, geram riscos maiores do que em outras áreas. Isto porque, em primeiro lugar, no mais das vezes os objetos de IoT são compactos, sendo necessária a instalação de *chips* de tamanho reduzido, o que dificulta a capacidade de processamento dos mesmos. Em segundo, grande parte desses chips não são desenvolvidos para terem atualizações rotineiras o que, no âmbito da *internet*, se torna uma grande falha de segurança. Em terceiro, a ausência de uma *expertise* de grande parte das empresas na área de desenvolvimento de *softwares* e *hardwares* de alto nível também enfraquece a segurança (Magrani, 2018, p. 95).

Mas mesmo assim, dispositivos de IoT fabricados por grandes empresas com altos investimento em segurança, em *hardware* e *software*, também são alvos de falhas e incidentes de segurança.

> O analista David Jacoby, da Kaspersky Lab, testou alguns aparelhos domésticos e detectou falhas que permitiram o acesso remoto às televisões. Isso se tornou mais preocupante desde a descoberta de que as smart TVs da Samsung capturavam as conversas de pessoais dos

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

> usuários utilizando sua funcionalidade de ativação por voz e coletavam o histórico de programas assistidos, tudo isso sem a permissão do consumidor (Magrani, 2018, p. 94).

Outro problema bastante frequente tanto em dispositivos de IoT quanto em qualquer outro serviço utilizado por usuários, é a utilização de senhas padrões, de fácil acesso por parte de terceiros. Um importante exemplo é o site *Insecam*, o qual apresenta milhares de câmeras de todos os lugares do globo terrestres, às quais se obteve acesso apenas com a utilização de senhas padrões. O objetivo desse site é o de alertar as pessoas sobre os perigos da utilização de dispositivos eletrônicos de filmagem sem que se tenham os cuidados mínimos de segurança inerentes (Magrani, 2018, p. 96).

Nessa seara, já no ano de 2016, o MCFAEE Labs lançou em seu relatório trimestral com previsões e perspectivas sobre a mitigação da privacidade em razão do grande aumento de dispositivos de IoT.

> Relatos sobre o fim da privacidade foram exagerados no passado, mas a IoT vai tornar esse fim mais próximo. Existem simplesmente dispositivos IoT demais observando, ouvindo, gravando, acumulando e acompanhando de outras formas o comportamento do consumidor. Em muitos casos, os consumidores pagam a uma empresa por um serviço e se permitem ser rastreados gratuitamente. É verdade que os detalhes estão nos contratos de licença do usuário, mas a maioria dos consumidores não os lê e não consegue evita-los, de qualquer forma. Os dispositivos Iot estão ultrapassando rapidamente os limites das atuais leis de privacidade e as instituições políticas continuarão a reagir lentamente. As expectativas de privacidade afetarão fornecedores de dispositivos e operadores de serviços, pois alguns governos exigirão contratos explícitos, adesões e até mesmo compensações pelo uso ou compartilhamento dos dados de alguém. (Magrani, 2019, p. 71).

Assim, a coleta de dados pessoais por meio de dispositivos da internet das coisas, para fins de utilização em algoritmos, tem encontrado seu sentido na medida “em que a cultura algorítimica vai constituindo um “segundo eu”, uma antena interfaciadora de dados, que conforme sugeriu Pablo Rodríguez, podemos denominar como subjetivação smartiphónica”. (Vilalta, 2020). Isto porque, os algoritmos criam uma

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

imagem de que temos acesso a tudo, mas que em verdade, personalizam dados "por meio de medidas estatísticas que não tem nada de pessoal. Criam nos sujeitos a ilusão de uma singularidade que é efeito da estatística, e esta, por sua vez, é efeito de um processamento da informação."(Vilalta, 2020).

Os problemas inerentes a estas novas tecnologias não param por ai, pois a capacidade inventiva e o crescente aumento do número de produtos cada vez mais tecnológicos e que prometem facilidades e comodidades para as atividades diárias, estão direta e proporcionalmente ligadas ao aumento de falhas de segurança e de vazamento de dados dos usuários para os mais diversos fins. Dessa forma, se faz necessário que o comprometimento das próprias empresas e zelar e informar os usuários dos riscos inerentes, sob pena de possíveis responsabilizações.

4 CONSIDERAÇÕES FINAIS

Diante do exposto, é possível se destacar que o direito à privacidade é um direito fundamental que foi sendo construído ao longo do tempo, com assento histórico no iluminismo. Tal direito se encontra elencado no rol dos direitos de primeira dimensão, sendo uma garantia dos cidadãos quanto a não interferência do Estado e de terceiros em referidos direitos. Os avanços tecnológicos, que passaram a ser introduzidos na sociedade, trouxeram uma gama de modificações nas relações sociais e, sobretudo, na forma como os cidadãos se comunicam e utilizam esses meios no dia a dia.

A utilização dos meios de comunicação (em especial a *internet*) e dos dispositivos de IoT, representam no contexto da atualidade uma importante mitigação ao direito à privacidade, haja vista que os usuários (quer de forma voluntária, ou mesmo de forma involuntária), passaram a compartilhar uma gama de dados privados com esses dispositivos. Mas não apenas isso, também se verifica que há o risco do próprio vazamento ou hackeamento dos aludidos dados por parte de terceiros, o que também importa em relevante prejuízo à privacidade dos usuários.

Todavia, pensar em uma sociedade descolada dos inúmeros dispositivos existentes da internet das coisas cada vez mais correlacionados aos mais diversos

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

produtos (e que por isso mesmo despontam na atenção dos usuários pela interconectividade com as inúmeras plataformas e aplicações existentes), se mostra um retrocesso impensável e inviável na atualidade.

Assim, se faz necessário que haja um ponto de equilíbrio entre a velocidade e inovações que os avanços relativos à Internet das Coisas trazem com os cuidados inerentes aos direitos da privacidade dos usuários. E tal necessidade exsurge a fim de que os usuários possuam os esclarecimentos necessários e a exata noção sobre o alcance do compartilhamento de seus dados, para fins de poderem optar e verificar o que pretendem ou não disponibilizar ao compartilhamento com as empresas responsáveis pelos dispositivos responsáveis pelas coletas e processamento de dados.

Nessa toada, e por meio dessas formas de esclarecimentos e transparente relação entre os usuários e as plataformas sobre como se dá (e como se dará) a coleta, o tratamento e a utilização dos dados pessoais, é que se torna possível uma utilização segura e eficaz dos inúmeros dispositivos da Internet das Coisas, característicos da internet 3.0.

REFERÊNCIAS

BAUMAN, Zygmunt. **Modernidade Líquida.** São Paulo: Zahar, 2010.

BRASIL. Constituição da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 08 set. 2023.

CARDOSO, *Carlos.* **Internet das coisas inúteis:** suporte de papel-higiênico conectado. Meiobit. Disponível em: https://meiobit.com/396909/internet-das-coisas-inuteis-suporte-de-papel-higienico-conectado/ Acesso em 08 set. 2023.

CASTELLS, Manuel. **A sociedade em rede.** São Paulo: Paz e Terra, 2005.

COMPARATO, Fábio Konder. **A afirmação histórica dos Direitos Humanos.** São Paulo: Saraiva, 2003

LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (Orgs.) Direito, processo e tecnologia. São Paulo: **Revista dos Tribunais**, 2020.

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

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p199-214

MAGRANI, Eduardo **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélago, 2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** Disponível em: https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humanos Acesso em: 08 set. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS **Pacto Internacional sobre Direitos Civis e Políticos.** Disponível em: https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20os%20Direitos%20Econ%C3%B3micos,%20Sociais%20e%20Culturais.pdf Acesso em: 08 set. 2023.

PAESANI, Liliana Minardi. **Direito e Internet:** Liberdade de informação, privacidade e responsabilidade civil. 7ª Edição. São Paulo, Atlas, 2014.

ROMERO, Luiz. Não Li e Concordo. **Revista Superinteressante**, 17 Mar 2017. Disponível em: https://super.abril.com.br/tecnologia/nao-li-e-concordo/ Acesso em: 08 set. 2023.

SANTOS, Bruno P.; SILVA, Lucas A. M.; CELES, Clayson S. F. S.; BORGES NETO, João B.;, VIEIRA, Marcos Augusto M.; VIEIRA, Luiz Felipe M.; GOUSSEVSKAIA, Olga N.; LOUREIRO, Antonio A. **Internet das Coisas:** da teoria à prática. Belo Horizonte: UFMG, 2016. Disponível em: https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf Acesso em: 08 set. 2023.

SARLET. Ingo Wolfgang. **A eficácia dos Direitos Fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2012.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 38. ed. São Paulo: Malheiros, 2015.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação:** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

VÉLIZ, Carissa. **Privacidade é poder:** Porque e como você deveria retomar o controle de seus dados. 1º Edição. São Paulo: Contracorrente, 2021.

VILALTA, Lucas Paolo. O neoliberalismo é uma governabilidade algorítimica. *In* **Revista Lacuna,** 27 de julho de 2020, nº 9. Disponível em: https://revistalacuna.com/2020/07/27/n-9-07/ Acesso em: 08 set. 2023.

ZANON, João Carlos. **Direito à proteção dos dados pessoais.** São Paulo, Revista dos Tribunais, 2013.