

UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Eduardo Missau Ruviaro

**(DES) PROTEÇÃO DE DADOS E INTERNET DAS COISAS: OS
DESAFIOS À TUTELA DOS DADOS DE SAÚDE DE USUÁRIOS DE
DISPOSITIVOS DE IOT À LUZ DOS PRECEITOS DA LGPD**

Santa Maria, RS
2021

Eduardo Missau Ruviaro

**(DES) PROTEÇÃO DE DADOS E INTERNET DAS COISAS: OS DESAFIOS À
TUTELA DOS DADOS DE SAÚDE DE USUÁRIOS DE DISPOSITIVOS DE IOT À
LUZ DOS PRECEITOS DA LGPD**

Dissertação apresentada ao curso de Pós-graduação em Direito na área de concentração Direitos Emergentes na Sociedade Global da Universidade Federal de Santa Maria (UFSM, RS) como requisito parcial para obtenção do grau de **Mestre em Direito**.

Orientador: Prof. Dr. Rafael Santos de Oliveira

Santa Maria, RS
2021

Ruviaro, Eduardo Missau
(Des) proteção de dados e internet das coisas: os desafios à tutela dos dados de saúde de usuários de dispositivos de IOT à luz dos preceitos da LGPD / Eduardo Missau Ruviaro.- 2021.
129 p.; 30 cm

Orientador: Rafael Santos de Oliveira
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Ciências Sociais e Humanas, Programa de Pós-Graduação em Direito, RS, 2021

1. Internet das coisas 2. Dados pessoais sensíveis 3. Saúde 4. LGPD 5. Proteção de dados I. Santos de Oliveira, Rafael II. Título.

Sistema de geração automática de ficha catalográfica da UFSM. Dados fornecidos pelo autor(a). Sob supervisão da Direção da Divisão de Processos Técnicos da Biblioteca Central. Bibliotecária responsável Paula Schoenfeldt Patta CRB 10/1728.


Declaro, EDUARDO MISSAU RUVIARO, para os devidos fins e sob as penas da lei, que a pesquisa constante neste trabalho de conclusão de curso (Dissertação) foi por mim elaborada e que as informações necessárias objeto de consulta em literatura e outras fontes estão devidamente referenciadas. Declaro, ainda, que este trabalho ou parte dele não foi apresentado anteriormente para obtenção de qualquer outro grau acadêmico, estando ciente de que a inveracidade da presente declaração poderá resultar na anulação da titulação pela Universidade, entre outras consequências legais.

Eduardo Missau Ruviano

**(DES) PROTEÇÃO DE DADOS E INTERNET DAS COISAS: OS DESAFIOS À
TUTELA DOS DADOS DE SAÚDE DE USUÁRIOS DE DISPOSITIVOS DE IOT À
LUZ DOS PRECEITOS DA LGPD**

Dissertação apresentada ao curso de Pós-graduação em Direito na área de concentração Direitos Emergentes na Sociedade Global da Universidade Federal de Santa Maria (UFSM, RS) como requisito parcial para obtenção do grau de **Mestre em Direito**.

Aprovada em 27 de maio de 2021:



Rafael Santos de Oliveira, Dr. (UFSM)
(Presidente/Orientador)



Rosane Leal da Silva, Dr.^a (UFSM)
(Examinadora)



Thami Coyatti Piaia, Dr.^a (URI)
(Examinadora)

Santa Maria, RS
2021

DEDICATÓRIA

A meus pais, Adair Ruviano e Aldaci Terezinha Missau Ruviano,
a meus irmãos, Heloísa Missau Ruviano e Henrique Missau Ruviano,
e a minha namorada, Gabriela Bolson,
pessoas que, acima de qualquer coisa, procuram ser mais aos outros que a si
mesmos.

AGRADECIMENTOS

Primeiramente, agradeço a meus pais, Adair Ruviano e Aldaci Terezinha Missau Ruviano, por terem me concedido a oportunidade de estudar em uma universidade pública, gratuita e de qualidade, a universidade que os formou, formou a minha irmã e formou o meu irmão. Esta dissertação de mestrado somente nasceu porque é reflexo do relacionamento crítico sob o qual o Direito é visto por todos os discentes e docentes da Universidade Federal de Santa Maria em seus cursos de graduação e de pós-graduação. Obrigado, pai e mãe, por acreditarem em mim e por empregarem na sua criação todos os esforços que bem sei não foram fáceis e poucos para que se moldasse a minha formação da melhor maneira avistada. Igualmente, agradeço a meus irmãos, Heloísa Missau Ruviano e Henrique Missau Ruviano, exemplos de hombridade e esforço, de estudo e dedicação, de anseios e destemores, pessoas que a providência me regalou o dom de amar.

Igualmente, agradeço a minha namorada, Gabriela Bolson, por toda a compreensão, por todo o estímulo e por todo o incentivo para que esse trabalho monográfico tomasse luz. Obrigado por ser a paz das minhas ondas, e por ser o arpoador de meus objetivos. Igualmente, esta dissertação de mestrado somente nasceu porque bebeu no teu apoio incondicional.

Honradamente, agradeço a meu orientador, o Prof. Dr. Rafael Santos de Oliveira, pelo estímulo, pela compreensão, pelo auxílio e pela paciência, dedicando-se a orientar minhas ideias e a rumar este trabalho. Mais que um professor, é alguém que admiro por empreender, mesmo frente às sabidas dificuldades do ensino público, paixão na atividade que desempenha. É sedenta a academia por profissionais como o Prof. Rafael. Da mesma sorte agradeço aos meus professores do Programa de Pós-graduação em Direito da Universidade Federal de Santa Maria, porque cada palavra dada em cada debate construído auxiliou na confecção de cada um dos tijolos da edificação desse trabalho científico.

Agradeço também ao antes amigo que sócio Jonas Marchesan Sartori, por entender minhas ausências nos momentos em que a universidade me abrigou por tanto tempo quanto o próprio escritório.

Por derradeiro, agradeço a todos aqueles que, de forma direta ou indireta, contribuíram para a minha graduação e para a construção desta dissertação de mestrado. Obrigado.

Os artesões se dedicam de corpo e alma. Primo, os artesões fazem as coisas por razões existenciais primeiro, financeiras e comerciais depois. [...]. Tertio, os artesões injetam um pouco da própria alma em seu trabalho: não venderiam uma peça defeituosa ou mesmo de qualidade duvidosa, porque isso fere seu orgulho.

(TALEB, Nassim Nicholas. **Arriscando a própria pele:** assimetrias ocultas no cotidiano. São Paulo: Objetiva. p. 42)

RESUMO

(DES) PROTEÇÃO DE DADOS E INTERNET DAS COISAS: OS DESAFIOS À TUTELA DOS DADOS DE SAÚDE DE USUÁRIOS DE DISPOSITIVOS DE IOT À LUZ DOS PRECEITOS DA LGPD

AUTOR: Eduardo Missau Ruviaro
ORIENTADOR: Rafael Santos de Oliveira

O presente trabalho investiga qual é a contribuição dada pela Lei Geral de Proteção de Dados Pessoais, no Brasil, para a tutela dos riscos a que estão expostos os usuários de aplicações conectadas à *internet* das coisas que utilizam ferramentas que capturam dados de saúde. A LGPD atua preventiva ou reparadoramente aos danos potenciais da captura de dados de saúde por aplicações de *internet* das coisas? Buscou-se, dedutivamente, apontar como se deu a evolução do conceito de *internet* no mundo, com o surgimento da *internet* das coisas dentro do contexto da quarta geração da *web*. Conceituou-se o que é a *internet* das coisas, quais são as facilidades trazidas pelas aplicações conectadas à IoT como um tema, e os riscos a que os usuários desses dispositivos, especialmente aqueles que capturam dados pessoais sensíveis de saúde, como um problema. O sopesamento desse tema e desse problema, que culminou em uma sociedade de risco, dedutivamente fez ser necessário o surgimento de normas protetivas de dados pessoais, a fim de tutelar o direito dos titulares de dados frente às aplicações conectadas à IoT. Descreveu-se o surgimento das ditas gerações de normas protetivas de dados, desde sua primeira geração até a LGPD no auge da quarta fase de normas protetivas. Observou-se, desta forma, que, na quarta geração de normas, a autodeterminação informativa, positivada através da base legal do consentimento, fez com que a LGPD não fosse capaz de tutelar os direitos dos titulares de dados pessoais sensíveis de saúde, além da vagueza dos dispositivos positivados e da reprimenda das sanções administrativas pautadas. Quanto à metodologia, utilizou-se o método de abordagem dedutivo, partindo-se da evolução do conceito de *internet* e de *internet* das coisas, sob o marco teórico de Castells e Magrani, passando pela sociedade de risco de Ulrich Beck, transitando pelo surgimento e pela importância das normas protetivas de dados, sob a doutrina de Doneda e Viktor Mayer-Schöenberger, ao que se pode responder, no último tópico do texto, efetivamente o problema de pesquisa. Como resultado se apontou a vinculação repressiva, e não preventiva, da Lei Geral de Proteção de Dados, na tutela do mal uso de dados pessoais sensíveis de saúde coletados a partir de aplicações de IoT, além da insuficiência da base legal do consentimento e da vagues das bases legais específicas, possibilitando o tratamento e o compartilhamento dos referidos dados pessoais.

Palavras-chave: Internet das coisas. Dados pessoais sensíveis. Saúde. LGPD. Proteção de dados.

ABSTRACT

DATA (UN) PROTECTION AND INTERNET OF THINGS: THE CHALLENGES FOR THE HEALTH DATA PROTECTION THROUGH IOT USERS' DEVICES IN THE LIGHT OF LGPD PRECEPTS

AUTHOR: Eduardo Missau Ruviaro

ADVISER: Rafael Santos de Oliveira

The present work investigates what is the contribution given by the General Law of Protection of Personal Data, in Brazil, for the protection of the risks to which the users of applications connected to the internet of the things that use tools that capture health data are exposed. Does LGPD act preventively or remedially to the potential damage caused by the capture of health data by IoT applications? We sought, deductively, to point out how the concept of internet in the world evolved, with the emergence of the internet of things within the context of the fourth generation of the web. It was conceptualized what is the internet of things, what are the facilities brought by applications connected to the IoT as a theme, and the risks to which the users of these devices, especially those that capture sensitive personal health data, as a problem. The weighing of this theme and this problem, which culminated in a risk society, deductively made it necessary for the emergence of protective norms of personal data, in order to protect the right of data subjects in the face of applications connected to the IoT. The emergence of the said generations of protective data standards was described, from its first generation to the LGPD at the height of the fourth phase of protective standards. It was observed, therefore, that, in the fourth generation of norms, informative self-determination, made positive by the legal basis of consent, made LGPD unable to protect the rights of holders of sensitive personal health data, in addition to the vagueness of the positive provisions and the reprimand of the guided administrative sanctions. As for the methodology, the deductive approach method was used, starting from the evolution of the concept of internet and internet of things, under the theoretical framework of Castells and Magrani, passing through Ulrich Beck's risk society, passing through the emergence and due to the importance of data protection rules, under the doctrine of Doneda and Viktor Mayer-Schöenberger, to which the research problem can be answered, in the last topic of the text. As a result, the repressive, and not preventive, link of the General Data Protection Law was pointed out, in the protection of the misuse of sensitive personal health data collected from IoT applications, in addition to the insufficiency of the legal basis of consent and vagues. specific legal bases, enabling the processing and sharing of said personal data.

Keywords: Internet of things. Sensitive personal data. Health. LGPD. Data protection

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
ANS	Agência Nacional de Saúde Suplementar
ARPA	Advanced Reserarch Projects Agency
CDC	Código de Defesa do Consumidor
CEMADEC	Centro de Monitoramento e Alarme da Defesa Civil
CGM	Continuous Glucose Monitor
CNA	Capacidade Nacional de Absorção
GDPR	General Data Protection Regulation
IOT	Internet of Things (Internet das Coisas)
IPTO	Information Processing Techniques Office
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
PIA	Privacy Impact Assessments
RGPD	Regulamento Geral de Proteção de Dados

SUMÁRIO

1 INTRODUÇÃO	11
2 A INTERNET DAS COISAS DENTRO DA SOCIEDADE DE RISCO: COMO A IOT POTENCIALIZA A FUGA DA PRIVACIDADE SOB A CORTINA DA AUTOMAÇÃO	17
2.1 INTERNET DAS COISAS COMO FERRAMENTA DA MODERNIDADE: FACILIDADES E DESAFIOS DOS OBJETOS INTELIGENTES	18
2.2 SOCIEDADE DE RISCO VIRTUALMENTE CONECTADA: TEMAS E PROBLEMAS DA INTERNET DAS COISAS EM APLICAÇÕES DE SAÚDE	43
3 AS GERAÇÕES DE NORMAS PROTETIVAS DE DADOS E O CASO BRASILEIRO: COMO A LGPD TRATA OS DADOS PESSOAIS SENSÍVEIS DE SAÚDE COLHIDOS A PARTIR DA INTERNET DAS COISAS?	71
3.1 PROTEÇÃO DE DADOS E CIBERESPAÇO: O MODELO DE REGULAMENTAÇÃO EUROPEU E O CASO BRASILEIRO	72
3.2 TUTELA DOS DADOS PESSOAIS SENSÍVEIS DE SAÚDE NA LEI GERAL DE PROTEÇÃO DE DADOS: PREVENÇÃO OU REPARAÇÃO?	96
4 CONCLUSÃO	115
REFERÊNCIAS	121

INTRODUÇÃO

A evolução inovadora das novas tecnologias, especialmente aquelas associadas à rede mundial de computadores, trouxe inúmeros benefícios aos usuários da *internet*. Desde a simplificação na troca de mensagens de texto até o barateamento de produtos e serviços, a *web* passou a desempenhar um papel de facilitadora da vida dos internautas. Com o desenvolvimento e com uma maior ramificação da utilização da rede mundial de computadores, a *internet*, em tese, democratizou-se, sendo, portanto, consumida por significativa parcela da população mundial. Como consequência disso, maior se tornou a dependência do até então mundo físico, analógico e desconectado à conectividade das aplicações ligadas à *web*, e mais serviços passaram a ser ofertados através das interligações da teia.

Nesse sentido, um dos caminhos lógicos atingidos pela evolução da rede é o surgimento da *internet* das coisas (IoT), ou seja, a comunicação máquina com máquina, através de inteligência artificial, buscando, sem interferência humana, a tomada de decisões em prol de seus usuários. Os exemplos de aplicações conectadas à *internet* das coisas são muitos, e cada vez mais diversificados. Desde *gadgets* alocados junto ao corpo humano, como *smartwatches* e *smartbands*, até carros inteligentes, a *internet* das coisas automatizou as pessoas, suas casas, e, de um modo geral, as grandes cidades ao redor do planeta.

Importantes ferramentas que passaram a ser valiosamente utilizadas sob o condão da *internet* das coisas são as aplicações que se ligam ao controle da saúde dos usuários. A conexão máquina com máquina, como forma de se buscar os cuidados com a saúde, fez com que fosse possível, aos usuários de aplicações conectadas à *internet* das coisas, o controle em tempo real de batimentos cardíacos, oxigenação sanguínea, atividades físicas, peso, índice de massa corporal, altura, alimentação, hidratação, consumo de fármacos, e até mesmo o funcionamento regular do coração, isto é, os principais elementos da procura por uma vida saudável. Essa automatização se faz através de aplicações conectadas à *internet* das coisas, como, por exemplo, *smartwatches* e *smartbands*, marca-passo inteligente, hospitais automatizados e mesmo detectores de cânceres automatizados, todos mecanismos que capturam os dados dos usuários, através de inteligência artificial, e, ao realizar o tratamento dessas informações, as

disponibilizam em bancos de dados conectados à *internet* para o fácil acesso dos usuários titulares e dos membros do sistema de saúde a esses dados de qualquer hora e a qualquer lugar.

Em razão disso, tudo o que, em busca de uma perfectibilização da saúde, antes era feito de maneira desconectada passou a percorrer um novo caminho na busca pela concretude de sua função, isto é, o que antes era analógico agora surfa na onda do digital, sendo a *internet* seu veículo locomotor. E as pegadas deixadas por esse novo meio de condução informacional, diferentemente do que se percebia no universo desconectado, são difíceis de serem apagadas. Não bastasse isso, se maior é a versatilidade do uso da *internet*, mais largo é o número de rastros que a rede mundial de computadores produz. Então, o grande uso da *web*, especialmente fomentado pela *internet* das coisas, passou a produzir incontável entrelaçamento de dados que antes não eram tão facilmente confeccionados. Assim, a *internet*, que em outro tempo era fomentada pelas pessoas, tornou-se das coisas, e os dados, que antes eram criados em menor escala no mundo *off-line*, passaram a ser vistos como as grandes *commodities* da atualidade.

O que pouco se atenta, nessa perspectiva, é que as aplicações conectadas à *internet* das coisas, especialmente aquelas vinculadas à saúde, arquetam os dados de seus usuários ininterruptamente. Essa engenharia, que mapeia as informações pessoais dos usuários das aplicações vinculadas à *internet* das coisas, não se manifesta de forma explícita, ao que, sorrateiramente, permite o tratamento silencioso dos dados que armazena. Como regra geral, são poucos os usuários que se preocupam com a captura de seus dados pessoais, fazendo com que, de saúde, as aplicações da *internet* das coisas por um lado ajudem na busca por uma melhor qualidade de vida física, mas, por outro lado, adoeçam a privacidade. Assim, enquanto a *internet* das coisas se vende como um mecanismo de importante auxílio na busca por um melhor desenvolvimento da saúde de seu usuário, por outro lado se mostra como uma verdadeira protagonista em uma sociedade de risco, demonstrando a fragilidade com que se expõe o titular dos dados pessoais a potenciais danos não declarados, através de um uso oculto das informações colhidas através da IoT, necessitando-se de novos mecanismos preocupados com a proteção dos titulares desses dados.

Em razão também disso, passou a surgir, ao redor do globo, modelos legislativos com o objetivo de proteger os dados pessoais de seus cidadãos.

Exemplo recente é a vigência da Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira, que tomou como inspiração o Regulamento Geral Sobre a Proteção de Dados (RGPD) europeu. A LGPD possui, dentre as suas bases legais, especialmente no inciso I do seu artigo 11, a autorização para o tratamento de dados pessoais na hipótese de proteção da vida ou da incolumidade física do titular dos dados ou de terceiro. Contudo, a legislação protetiva de dados pessoais não estabelece limites para o tratamento dos dados quando o assunto for a busca pela saúde, o que pode – ou não – tornar vulnerável o direito à privacidade dos usuários de aplicações conectadas à *internet* das coisas que capturem esses dados sensíveis de saúde.

Diante disso, a presente dissertação questiona qual é a contribuição da Lei Geral de Proteção de Dados Pessoais no Brasil para tutelar os riscos a que estão expostos os usuários de aplicações conectadas à *internet* das coisas que utilizam ferramentas que capturam dados de saúde? Nesse novo contexto, onde os riscos são potencializados pelas redes, a LGPD atua preventiva ou reparadoramente aos danos potenciais da captura de dados de saúde por aplicações de IoT? Para responder a esse problema de pesquisa, utiliza-se duas teorias de base, ou seja, alicerces teóricos destinados a dar sustento para a interpretação do que se propôs desenvolver na investigação. Essas teorias de base são a da proteção de dados pessoais, através de autores que se encaixam perfeitamente à temática da pesquisa desenvolvida, principalmente porque se baseia em investigações que acompanharam todo o desenvolvimento histórico da *internet*, estando, portanto, aptas a dialogar com os novos desafios que a rede mundial de computadores – e, portanto, a *internet* das coisas – está por atravessar, e a da sociedade de risco.

A primeira teoria de base é a da proteção de dados. A teoria de base da proteção de dados se justifica tendo em vista que, para que pudesse responder ao problema de pesquisa, é fundamental aprofundar-se no conceito de *internet* das coisas e, conseqüentemente, da proteção de dados pessoais. E pode-se considerar como aplicação conectada à *internet* das coisas aquelas em que há contato *machine-to-machine* para satisfazer as necessidades humanas, ou seja, exatamente o propósito do surgimento da *internet* como rede mundial de computadores. Antes da compreensão de o que é *internet* das coisas, portanto, é vital que se compreenda qual é a sociedade da informação. Assim, a utilização de autores como Castells, Berners-Lee, Pérez Luño e Pyerre Levy, que compõe importante gama de pesquisas

que tratam do surgimento e desenvolvimento da *web*, é caminho teórico importante para a boa compreensão da dialética desse esboço. Especialmente no que toca à *internet* das coisas, se vale dos estudos de Magrani, Lemos e Ashton, além de outras publicações, para embasar a pesquisa dessa parte do trabalho.

Um dos autores-chave para compreensão da teoria da privacidade e proteção de dados pessoais é Doneda que, ao lado de outros como Pasquale, Magrani e Fortes, é essencial para a compreensão de que a proteção de dados deve ser entendida como um direito inegociável na *internet* das coisas, especialmente porque decorre da proteção à privacidade. Ainda, continua-se utilizando tal teoria ao realizar a narrativa, por Mayer-Schöenberger e Doneda, de como se deu a evolução histórica das gerações de leis gerais de proteção de dados pessoais ao redor do globo. Já a segunda teoria de base, da compreensão da sociedade de risco, é referenciada por Ulrich Beck.

A pesquisa tem por objetivo geral investigar como a Lei Geral de Proteção de Dados Pessoais brasileira pode contribuir, se preventiva ou reparadoramente, para a proteção dos dados pessoais sensíveis de saúde dos titulares usuários de aplicações conectadas à *internet* das coisas. Para tanto, como objetivos específicos elencou-se, em um primeiro momento, classificar a IoT dentro de um contexto de desenvolvimento da *internet*, descrever quais são os possíveis danos decorrentes da má utilização de disposições de IoT vinculadas à saúde em uma sociedade do risco, mapear o surgimento das normas protetivas de dados, bem como de suas gerações, ao redor do globo até o surgimento da LGPD e, finalmente, respondendo ao problema de pesquisa, identificar qual é a contribuição da LGPD no Brasil para tutelar os riscos a que estão expostos os usuários de IoT que utilizam ferramentas que capturam dados de saúde.

Como método de abordagem, essa investigação foi conduzida por linhas dedutivas. Esse método consiste na formulação de um problema de pesquisa, de forma clara e objetiva, cuja resposta se dá através do percurso de um caminho dedutivo, onde a conclusão é consequência do desenvolvimento investigativo empregado. No caso dessa dissertação, se aborda, dedutivamente, em primeiro lugar, a conceituação de *internet* das coisas, passando pela alocação da proteção de dados pessoais dentro de uma sociedade de risco, chegando à evolução legislativa para o surgimento da Lei Geral de Proteção de Dados Pessoais brasileira,

culminando na resposta, interpretativa ao texto legal, ao problema de pesquisa esboçado.

Deste modo, a fim de responder a essa indagação (o problema de pesquisa), partiu-se de uma investigação sobre o surgimento da rede mundial de computadores e, também, da IoT. É importante contextualizar o surgimento da *internet* (das coisas e das pessoas), com a conexão de computadores de forma *on-line*, porque o objetivo de seu desenvolvimento era de que, um dia, as decisões humanas pudessem ser tomadas de forma automatizada e inteligente pelas máquinas (ou ao menos induzidas pelas coisas aos seres humanos). Essa fase da *internet*, que fora concebida por Berners-Lee, chegou ao seu ápice na *web* 4.0 (ou 5.0, 6.0 7.0...), e, com o desenvolvimento da *internet* das coisas, passou a rede mundial de computadores a executar este seu objetivo fundamental. Assim, partindo do surgimento da proteção de dados pessoais, investiga-se o nascimento da *internet* das coisas, especialmente sob o prisma da proteção de dados de saúde capturados pela IoT, como nova era da *internet*.

Em decorrência da *internet* das coisas, por outro lado, tem-se como intrínseco a sua operacionalidade o tratamento e a utilização de dados pessoais da saúde. Dessa forma, a pesquisa, em sua segunda fase, trabalha, dentro do conceito de *internet* das coisas e dos dados pessoais sensíveis de saúde, o que são esses dados pessoais. Assim, após partir do nascimento da *internet* e, mais precisamente, da *internet* das coisas, passando pela proteção de dados de saúde e pela consequente evolução legislativa da tutela dos dados pessoais, busca responder especificamente ao problema de pesquisa sob o prisma da Lei Geral de Proteção de Dados Pessoais brasileira.

Como métodos de procedimento, na primeira fase da dissertação, utiliza-se os métodos de procedimento monográfico e tipológico. Assim, através do método de procedimento monográfico, descreve-se a evolução da *internet* e da *internet* das coisas. Já o método de procedimento tipológico é importante para mostrar como, num plano real, encontra-se a IoT dentro de uma sociedade de risco. Já na segunda etapa da investigação se utiliza o método de procedimento histórico para descrever como, faticamente, se deu a evolução do ordenamento jurídico protetivo de dados pessoais ao redor do globo e, precisamente, no Brasil, apontando, dedutivamente, como é aplicada a LGPD na tutela dos dados pessoais sensíveis de saúde coletados a partir de dispositivos conectados junto à aplicações de *internet* das coisas. Como

técnicas de pesquisa, por sua vez, a inspeção se vale das formas bibliográfica e documental. A primeira técnica de pesquisa, bibliográfica, é utilizada tendo em vista que se descreve, teoricamente, a *internet* das coisas e a privacidade no ciberespaço. Já a técnica de pesquisa documental se aplica para que se possa analisar o arcabouço jurídico pertinente à proteção de dados pessoais, a fim de investigar a (des) proteção de dados pessoais e os impactos sobre o direito à privacidade dos usuários de aplicações conectadas à *internet* das coisas e os dados pessoais sensíveis de saúde.

O presente trabalho se divide, assim, em dois capítulos, com dois subcapítulos cada um, estruturando-se de modo a percorrer todo o caminho que liga o surgimento da *internet* das coisas com o desenvolvimento da *internet* e, utilizando-se as disposições conectadas à IoT junto às necessidades médicas, e demonstrando como a captura de dados pessoais fez surgir a tribulação de se desenvolver legislações protetivas de dados pessoais, como a LGPD brasileira, sendo essas, assim, as pretensas atrizes responsáveis pela tutela dos dados pessoais sensíveis de saúde oriundos a partir da capturas de dados pessoais por aplicações de *internet* das coisas. Portanto, como a Lei Geral de Proteção de Dados Pessoais brasileira pode contribuir, se preventiva ou reparadoramente, para a proteção dos dados pessoais sensíveis de saúde dos titulares usuários de aplicações conectadas à *internet* das coisas, é o que se responderá a partir de agora.

2 A INTERNET DAS COISAS DENTRO DA SOCIEDADE DE RISCO: COMO A IOT POTENCIALIZA A FUGA DA PRIVACIDADE SOB A CORTINA DA AUTOMAÇÃO

O desenvolvimento e o aperfeiçoamento da *internet*, ao longo dos anos, fez com que uma sociedade completamente analógica se transformasse em uma verdadeira comunidade da emergência. E essa emergência, que emana do cerne da rede mundial de computadores, trouxe consigo a necessidade perene de, cada vez mais, as máquinas ou tomarem ou induzirem decisões humanas, de modo a dinamizar e agilizar uma vida que, digitalmente, mostrou-se ser extremamente imediata. Dessa forma, o desenvolvimento da *web* pautou-se justamente em ensinar máquinas a comunicarem-se digitalmente com máquinas independentemente da vontade humana. A isso se deu o nome de *internet* das coisas.

Por outro lado, o novo andamento da *internet*, que das pessoas se transferiu às coisas, precisou, como contrapartida a esse avanço inventivo, capturar os dados pessoais desses usuários de aplicações conectadas à *internet* das coisas. Mais grave que isso é o inventário e a partilha de dados de saúde desses titulares, que são verdadeiros dados pessoais sensíveis, isto é, hábeis a identificar e mapear quem são seus detentores. De posse desses dados pessoais sensíveis de saúde, inúmeros são os danos a que potencialmente podem se sujeitar esses titulares de dados. Consequentemente, nesse contexto, inseriu-se a IoT dentro de uma verdadeira sociedade de risco, isto é, imersa em um universo em que o uso obscuro dos dados pessoais sensíveis de saúde pode ocasionar um uso indevido desses dados pessoais. Se, de um lado, há as facilidades e os desafios dos objetos inteligentes ligados à saúde dos usuários de aplicações conectadas à *internet* das coisas, do outro lado há os temas e os problemas da IoT capturando esses mesmos dados pessoais sensíveis de saúde.

Assim, esse paradoxo da *internet* coloca em choque a proteção de dados pessoais com o desenvolvimento das aplicações de IoT que se valem de dados pessoais sensíveis de saúde de seus usuários. Portanto, a *internet* das coisas dentro da sociedade de risco pode apontar como a IoT potencializa a fuga da privacidade sob a cortina da automação, confrontando tema e problema, e sinalizando para os embates que o Direito travará sobre a matéria.

2.1 INTERNET DAS COISAS COMO FERRAMENTA DA MODERNIDADE: FACILIDADES E DESAFIOS DOS OBJETOS INTELIGENTES

A *internet* é instrumento que se modifica diariamente quando, a cada dia que passa, novas aplicações conectadas à rede mundial de computadores surgem para suprir inovadoras demandas do ciberespaço. Contudo, mesmo que hoje seja utilizada para as mais variadas tarefas da sociedade civil, nem sempre a *internet* fora acessível à população de modo geral – o que remonta especialmente ao seu surgimento. Para que se possa compreender a *internet* das coisas (e sua utilização com objetivo explícito de busca por um maior controle da saúde daquele que a utilizar) é basilar que se discuta, antes, o surgimento da rede mundial de computadores e o seu conseqüente lugar de fala. Isso porque, como diz Castells, “a história da criação e do desenvolvimento da *internet* é a história de uma aventura humana extraordinária”¹ que “ajuda-nos a compreender os caminhos de sua futura produção da história”². Para que se inteire do fim, antes é necessário se percorrer o meio. É o que se demonstrará.

A origem da *internet* pode ter como seu embrião o que ficou conhecido, em 1969, como Arpanet, isto é, “uma rede de computadores montada pela *Advanced Research Projects Agency*”³. Antes disso, contudo, ainda em 1958, a *Advanced Reserach Projects Agency*, ou ARPA, fora projetada pelo Departamento de Defesa dos Estados Unidos. O fim almejado por essa organização era uma missão para concentrar as investigações acadêmicas estadunidenses com o objetivo geral de superar, tecnologicamente, o poderio militar norte-americano em relação a então ainda existente União das Repúblicas Socialistas Soviéticas. Isso porque, então em 1957, a União Soviética lançou ao universo o primeiro satélite Sputnik, demonstrando sua avançada capacidade de inovação espacial.

Quando arremetido o primeiro satélite Sputnik ao espaço, no final dos anos 50, a Arpanet “não passava de um pequeno programa que surgiu de um dos departamentos da ARPA, o *Information Processing Techniques Office* (IPTO),

¹ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 13.

² *Idem.*

³ *Idem.*

fundado em 1962”⁴, tendo como objetivo “estimular a pesquisa em computação interativa”⁵. O que buscavam os pesquisadores da ARPA era especificamente “uma maneira de permitir aos vários centros de computadores e grupos de pesquisa que trabalhavam para a agência compartilhar *on-line* tempo de computação”⁶. Acontece que, ao desenvolver seus projetos, “a ARPA empreendeu inúmeras iniciativas ousadas, algumas das quais mudaram a história da tecnologia e anunciaram a chegada da Era da Informação”⁷. Uma dessas iniciativas, segundo Castells, foi a criação de um sistema, através de uma teia de computadores em rede, que se propunha ser inabalável por ataques nucleares⁸.

Isso porque, para montar essa rede interativa de computadores, aonde grupos de pesquisa poderiam compartilhar *on-line* seu tempo de computação, o *Information Processing Techniques Office* valeu-se de uma tecnologia que, àquela época, revolucionaria a transmissão de dados⁹ de uma forma nunca antes vista. Dita tecnologia era o que se conheceu por comutação por pacotes, uma arquitetura em rede desenvolvida em parceria entre a *Rand Corporation*, por Paul Baran, e o *British National Physical Laboratory*, por Donald Davies¹⁰. Segundo Castells,

o projeto de Baran de uma rede de comunicação descentralizada, flexível, foi uma proposta que a *Rand Corporation* fez ao Departamento de Defesa para a construção de um sistema militar de comunicações capaz de sobreviver a um ataque nuclear, embora esse nunca tenha sido o objetivo por trás do desenvolvimento da Arpanet. O IPTO usou essa tecnologia de comutação por pacote no projeto da Arpanet.¹¹

Com o objetivo de mobilizar recursos de pesquisa – especialmente universitária – para tornar o Departamento de Defesa dos Estados Unidos superior tecnologicamente em relação à União Soviética¹², após o lançamento do satélite Sputnik, permitindo que vários computadores pudessem trabalhar de forma compartilhada e *on-line*, a teia de computadores conectados da Arpanet fez surgir,

⁴ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 13-14.

⁵ *Ibidem.* p. 14.

⁶ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 14.

⁷ CASTELLS, Manuel. **A Sociedade em Rede**: volume 1. 8. ed. São Paulo: Paz e Terra, 2005. p. 82.

⁸ *Ibidem.* p. 83.

⁹ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 14.

¹⁰ *Idem.*

¹¹ *Idem.*

¹² *Idem.*

ainda em Castells, o que se conheceu como *Information Processing Techniques Office*¹³, em 1962. Essa rede interativa de computadores formada pelo IPTO “valeu-se de uma tecnologia revolucionária de transmissão de telecomunicações”¹⁴, descentralizando os dados alocados nas máquinas para o que posteriormente veio a ser conhecido como nuvem.

Todavia, foi somente em primeiro de setembro de 1969 que entrou em funcionamento a pioneira rede de computadores da Arpanet¹⁵. Castells afirma que, em 1969, os primeiros nós da rede estavam na Universidade da Califórnia, em Los Angeles e em Santa Barbara, e na Universidade de Utah¹⁶. Já em 1971, 15 anos após o início do projeto Arpanet, a maioria dos centros universitários de pesquisa norte-americanos já possuía um sistema de rede¹⁷ interligando seus computadores de forma *on-line*. E, após o projeto Arpanet passar a ser implementado por *Bolt, Beranek & Newman*, empresa estadunidense de engenharia acústica sediada em Boston, em 1972, teve sua primeira demonstração bem-sucedida em uma conferência internacional em Washington, capitaneada por pesquisadores da Universidade de Harvard e do Instituto de Tecnologia de Massachusetts¹⁸. Assim, o primeiro passo do que seria futuramente batizado de *internet* fora dado.

Ocorre que a Arpanet tornava possível tão somente a interconexão *on-line* de dispositivos acoplados ao sistema da própria Arpanet, sem a viabilidade de conexão com outros sistemas que pudessem surgir para o compartilhamento em teia, o que limitava o acesso a outras redes de computadores. Portanto, o próximo passo para o nascedouro da *internet* foi “tornar possível a conexão da Arpanet com outras redes de computadores”¹⁹, como, por exemplo, as demais redes administradas pela ARPA (PRNET e SATNET). Para Castells, essa era a introdução de um conceito de “rede de redes”²⁰, o que em 1973, foi objeto de análise por dois cientistas da computação da Universidade de Stanford:

¹³ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 13.

¹⁴ *Idem.*

¹⁵ CASTELLS, Manuel. **A Sociedade em Rede**: volume 1. 8. ed. São Paulo: Paz e Terra, 2005. p. 82-83.

¹⁶ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 14.

¹⁷ *Idem.*

¹⁸ *Idem.*

¹⁹ *Idem.*

²⁰ *Idem.*

Em 1973, dois cientistas da computação, Robert Kahn, da ARPA, e Vint Cerf, então na Universidade Stanford, escreveram um artigo delineando a arquitetura básica da *internet*. Basearam-se nos esforços do *Networking Group*, um grupo técnico cooperativo formado na década de 1960 por representantes dos vários centros de computação ligados pela Arpanet, com o próprio Cerf, Steve Crocker e Jon Postel, entre outros. Para que pudessem falar umas com as outras, as redes de computadores precisavam de protocolos de comunicação padronizados. Isso foi conseguido em parte em 1973 [...].²¹

Em um seminário realizado na Universidade de Stanford, conseguiu-se comunicar duas redes de computadores distintas, com um protocolo de comunicação padronizado chamado de protocolo de controle de transmissão (TCP)²². Posteriormente, em 1978, na Universidade da Califórnia do Sul, Cerf, Postel e Crocker, por sua vez, “dividiram o TCP em duas partes, acrescentando um protocolo intra-rede (IP), o que gerou o protocolo TCP/IP”²³. O padrão TCP/IP, criado em 1978, isto é, há mais de quatro décadas, é operado até hoje nas conexões entre computadores de diferentes redes.

Uma vez que completou seu objeto geral, que era concentrar investigações acadêmicas estadunidenses para superar, tecnologicamente, o poderio militar norte-americano em relação a então ainda existente União das Repúblicas Socialistas Soviéticas, a Arpanet, em 1975, foi transferida para a *Defense Communication Agency*²⁴. E então, em 1983, com a criação de um sistema independente para uso específico militar pelo Departamento de Defesa, “a Arpanet tornou-se ARPA-INTERNET, e foi dedicada à pesquisa”²⁵. Em 1990, o projeto Arpanet foi retirado de operação, porque se tornou tecnologicamente obsoleto, e, com a tecnologia de redes de computadores no domínio público, o governo dos EUA “tratou logo de encaminhar a privatização da *internet*”²⁶. Castells relata, ainda, que, em 1990 a “maioria dos computadores nos EUA tinha capacidade de entrar em rede, o que lançou os alicerces para a difusão da interconexão de redes”²⁷, abrindo caminho, em 1995, para a operação privada da *internet*.

²¹ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 14.

²² *Idem*.

²³ *Ibidem*. p. 14-15

²⁴ *Ibidem*. p. 15.

²⁵ *Idem*.

²⁶ *Idem*.

²⁷ *Idem*.

Desta forma, se de 1969 a 1995 a *internet* persistiu sendo utilizada para fins bélicos, com a possibilidade muito estreita da população civil se valer da rede mundial de computadores, no ano de 1995, frente ao fim das operações pela Arpanet, a *Internet* passou a fazer parte da sociedade civil organizada²⁸. Assim, de lá para cá, a rede mundial de computadores incorporou inúmeras mudanças, desde a conexão de forma discada passar a ser através de rede de banda larga e fibra ótica até mesmo a transformação da maneira de se comercializar, estudar e trabalhar. Contudo, mesmo se considerando o projeto Arpanet como um marco visceral para a criação da *internet*, o nascedouro da rede mundial de computadores pode não ter se dado exclusivamente pelos esforços empregados na Arpanet. Tanto é assim que “o que permitiu à *internet* abarcar o mundo todo foi o desenvolvimento da *www*”²⁹.

O sistema *www*, ou *world wide web*, é uma aplicação para compartilhamento de dados e informações desenvolvida em 1990 por Tim Berners-Lee, que, à época, trabalhava no Laboratório Europeu para a Física de Partículas, o CERN, em Genebra, na Suíça. Berners-Lee, ainda antes do surgimento da *web*, acreditava que, em tradução livre, “os computadores poderiam se tornar muito mais poderosos se eles pudessem ser programados para compartilhar informações de dispositivos não conectados”³⁰. Nas palavras de Berners-Lee,

Suponha-se que todas as informações arquivadas em computadores ao redor do globo estivessem lincadas. Eu penso. Suponha-se que eu pudesse programar o meu computador para criar um espaço no qual tudo poderia estar conectado a tudo. Todos os bites de informações em qualquer computador do CERN, e em qualquer computador do planeta, estariam à disposição para mim e para qualquer outra pessoa. Seria um espaço singular, um centro global de informações.³¹

A ideia de Berners-Lee era criar um sistema que fosse capaz de assistir a mente humana na solução intuitiva de seus problemas³². E a forma que o programador encontrou para criar esse sistema foi desenvolvida, inicialmente,

²⁸ CASTELLS, Manuel. **A Sociedade em Rede**: volume 1. 8. ed. São Paulo: Paz e Terra, 2005. p. 83.

²⁹ CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 17.

³⁰ BERNERS-LEE, Tim. **Weaving the Web**: the original design of the World Wide Web by its inventor. Cambridge: Haper Business, 1999. p. 4.

³¹ Tradução livre de: “Suppose all the information stored on computers everywhere were linked. I thought. Suppose I could program my computer to create a space in which anything could be linked to anything. All the bits of information in every computer at CERN, and on the planet, would be available to me and to anyone else. There would be a single, global information space”. *Idem*.

³² *Ibidem*. p. 5.

através do programa *Enquire*. Este programa, que foi desenvolvido depois da criação da *internet*, definiu e implementou o que permitiria obter e acrescentar informações em rede, de forma *on-line*, e de qualquer computador conectado na teia da *internet*. Isso somente foi possível através do surgimento das lincagens em HTTP, HTML e URL³³. Foi em 1990, contudo, que, segundo Castells, Burners-Lee, em colaboração a Robert Cailliau, “construiu um programa navegador/editor [...] e chamou esse sistema de hipertexto de *world wide web*, a rede mundial”³⁴. Assim se deu o nascedouro da *internet* e da *web*, a rede mundial de computadores.

Nesse sentido, a *web*, após sua inserção para uso pela sociedade civil organizada, passou por diversas eras de evolução. Essas fases articularam-se desde o que se concebeu por *web* 1.0 até a *web* 4.0 ou 5.0 (ou 6.0, ou 7.0, ou...), o atual estado da arte da sociedade em rede. A primeira era da *internet*, conhecida como “a *Web*”³⁵, dava conta de que a rede mundial de computadores servia como uma “ferramenta exclusiva para leitura e formação de cognição”, segundo Fuchs, Hofkirchner, Schafranekm Rafflm Sandoval e Bichler³⁶, ou seja, um instrumento de busca, sem a participação da sociedade. Conhecida como *read-only-web*, a primeira fase da rede surgiu como a significação do conceito de tecnologias da informação e da comunicação, haja vista que, como salienta Gil³⁷, passou-se a dispor de um vasto número de informações possível de ser consultado em qualquer hora do dia por qualquer usuário conectado à rede:

³³ BERNERS-LEE, Tim. **Weaving the Web: the original design of the World Wide Web by its inventor**. Cambridge: Haper Business, 1999. p. 2.

³⁴ CASTELLS, Manuel. **A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003. p. 18.

³⁵ NAIK, Umesha; SHIVALINGAIAH, D. Comparative Study of Web 1.0, Web 2.0 and Web 3.0. In: 6° INTERNATIONAL CALIBER, 6., 2008, Allahabad. **Anais 6° International CALIBER**. Allahabad: Infflibnet Centre, 2008. v. 1, p. 499-507. Disponível em: <https://ir.infflibnet.ac.in/bitstream/1944/1285/1/54.pdf>. Acesso em: 22 abr. 2020.

³⁶ Tradução livre de: “Accordingly, we define Web 1.0 as a tool for cognition”. FUCHS, Christian et al. Theoretical Foundations of the Web: Cognition, Communication, and Co-Operation. Towards an Understanding of Web 1.0, 2.0, 3.0. **Future Internet**, [S.l.], v. 1, n. 2, p. 41-59, fev. 2010. Disponível em: https://www.researchgate.net/publication/41667703_Theoretical_Foundations_of_the_Web_Cognition_Communication_and_Co-Operation_Towards_an_Understanding_of_Web_10_20_30. p. 43. Acesso em: 11 jun. 2019.

³⁷ GIL, Henrique Teixeira. A passagem da Web 1.0 para a Web 2.0 e... Web 3.0. **Instituto Politécnico de Castelo Branco: potenciais consequências para uma humanização em contexto educativo**. Castelo Branco, p. 1-2. mar. 2014. Disponível em: <https://repositorio.ipcb.pt/bitstream/10400.11/2404/1/A%20passagem%20da%20Web%20Henrique.pdf>. Acesso em: 22 abr. 2020.

Com a utilização da *internet*, na sua fase inicial que poderá ser chamada de *Web 1.0*, foi criado um novo contexto, um contexto de abertura que justificou o aparecimento de um novo conceito e de acrónimo: Tecnologias da Informação e da Comunicação – TIC. Nesta 1ª geração da *Web* as utilizações eram do tipo *read-only web* onde as operações de *download* eram a imagem de marca da sua utilização estando tudo ao alcance do também designado efeito de *fangertips*. Neste contexto, estamos a falar de uma verdadeira Sociedade da Informação pelo facto de passarmos a dispor de um autêntico caldo de informação onde tudo se podia consultar a qualquer hora do dia³⁸.

Por outro lado, embora possa ser considerada com um marco importante para a democratização do acesso à informação, Naik e Shivaligaiah afirmam que, na *web 1.0*, um pequeno número de escritores estava apto a criar as páginas da *internet* para que um grande número as consumisse diariamente. Naik e Shivaligaiah ainda sustentam que, embora temporalmente situada com início em 1995, desde a privatização da *internet*, teve acesso consolidado por 45 milhões de usuários ao redor do mundo em 250 mil sítios eletrônicos³⁹. Conforme articula Gil, a *web 1.0*, por sua vez, durou desde a privatização da *internet*, em 1995, até aproximadamente 2005⁴⁰, com sua superação completa.

Já a segunda era da *internet* foi definida por Fuchs, Hofkirchner, Schafranekm Raffm Sandoval e Bichler como uma *web* de leitura e escrita⁴¹, na qual os atores do ciberespaço poderiam, além de colher informações e formar sua convicção, estruturar a arquitetura da *internet*. A passagem da *web 1.0* para a *web 2.0* significou em uma alteração drástica na forma como os usuários puderam lidar com a teia, tendo em vista que, para Gil, as novas ferramentas digitais assentavam-se

³⁸ GIL, Henrique Teixeira. A passagem da Web 1.0 para a Web 2.0 e... Web 3.0. **Instituto Politécnico de Castelo Branco: potenciais consequências para uma humanização em contexto educativo**. Castelo Branco, p. 1-2. mar. 2014. Disponível em: <https://repositorio.ipcb.pt/bitstream/10400.11/2404/1/A%20passagem%20da%20Web%20Henrique.pdf>. Acesso em: 22 abr. 2020.

³⁹ NAIK, Umesha; SHIVALINGAIAH, D. Comparative Study of Web 1.0, Web 2.0 and Web 3.0. In: 6º INTERNATIONAL CALIBER, 6., 2008, Allahabad. **Anais 6º International CALIBER**. Allahabad: Infflibnet Centre, 2008. v. 1, p. 499-507. Disponível em: <https://ir.infflibnet.ac.in/bitstream/1944/1285/1/54.pdf>. Acesso em: 22 abr. 2020.

⁴⁰ GIL, Henrique Teixeira. A passagem da Web 1.0 para a Web 2.0 e... Web 3.0. **Instituto Politécnico de Castelo Branco: potenciais consequências para uma humanização em contexto educativo**. Castelo Branco, p. 1-2. mar. 2014. Disponível em: <https://repositorio.ipcb.pt/bitstream/10400.11/2404/1/A%20passagem%20da%20Web%20Henrique.pdf>. Acesso em: 22 abr. 2020.

⁴¹ FUCHS, Christian et al. Theoretical Foundations of the Web: Cognition, Communication, and Co-Operation. Towards an Understanding of Web 1.0, 2.0, 3.0. **Future Internet**, [S.l.], v. 1, n. 2, p.41-59, fev. 2010. Disponível em: https://www.researchgate.net/publication/41667703_Theoretical_Foundations_of_the_Web_Cognition_Communication_and_Co-Operation_Towards_an_Understanding_of_Web_10_20_30. Acesso em: 11 jun. 2019.

“num novo conceito, o conceito de partilhar”⁴². Gil ainda sustenta que, na *web* social, a 2ª geração da *web*, começou-se a adotar interações do tipo *read-write*, aonde os usuários da rede eram capazes de criar os conteúdos escritos para o consumo dos próprios usuários, de forma mais democrática e mais plural. Como exemplo, Gil traz as redes sociais *Linkedin*, *Orkut*, *Facebook* e *Twitter*⁴³. Contudo, foi na *web* 2.0 que se iniciou a transmissão e partilha de dados pessoais. É o que afirma ao dizer que o “êxito desta rede social digital prende-se com o facto [sic] de potenciar e de estimular a partilha de dados e de informações”⁴⁴. Gil ainda sustenta que, com o compartilhamento de dados e informações pessoais, a *web* tornou-se social, humanizando-se as relações entre os diferentes dispositivos conectados à rede⁴⁵. Por essa razão, foi consequência dos dados compartilhados “a discussão e reflexão crítica que lhe é subjacente”⁴⁶, criando “condições para se poder afirmar que se promove a passagem de uma Sociedade da Informação para a Sociedade do Conhecimento”⁴⁷. A *web* 2.0 contou, segundo apurou Naik e Shivalingaiah⁴⁸, com aproximadamente 80 milhões e sítios eletrônicos, e, entre 2000 e 2010, quando se superou completamente sua exposição, foi acessada por mais de 1 bilhão de usuários ao redor do planeta. A *web* 2.0 foi suplantada pelas *web* 3.0, 4.,0 e 5.0 (ou 6.0, ou 7.0, ou...), o atual estado da arte das redes de dispositivos conectados de forma *on-line*.

Por sua vez, a terceira era da *internet* é chamada de *web* semântica. Esse batismo se justifica porque possui como característica fundamental “a inserção e consolidação da tecnologia da inteligência artificial, *machine learning* e algoritmos de personalização baseados na coleta de dados pessoais do usuário na experiência de navegação”⁴⁹. Na *web* semântica, é o usuário do ciberespaço quem alimenta, edita,

⁴² GIL, Henrique Teixeira. A passagem da Web 1.0 para a Web 2.0 e... Web 3.0. **Instituto Politécnico de Castelo Branco: potenciais consequências para uma humanização em contexto educativo**. Castelo Branco, p. 1-2. mar. 2014. Disponível em: <https://repositorio.ipcb.pt/bitstream/10400.11/2404/1/A%20passagem%20da%20Web%20Henrique.pdf>. Acesso em: 22 abr. 2020.

⁴³ *Idem*.

⁴⁴ *Idem*.

⁴⁵ *Idem*.

⁴⁶ *Idem*.

⁴⁷ *Idem*.

⁴⁸ NAIK, Umeha; SHIVALINGAIAH, D. Comparative Study of Web 1.0, Web 2.0 and Web 3.0. In: 6° INTERNATIONAL CALIBER, 6., 2008, Allahabad. **Anais 6° International CALIBER**. Allahabad: Inflibnet Centre, 2008. v. 1, p. 499-507. Disponível em: <https://ir.inflibnet.ac.in/bitstream/1944/1285/1/54.pdf>. Acesso em: 22 abr. 2020.

⁴⁹ SANGOI, Rafael Martins. **A Necessidade de Adaptação do Direito ao Tempo da Internet: desafios e perspectivas para a cidadania digital contemporânea**. 2019. 120 f. Dissertação (Mestrado)

armazena e fomenta os dados e as informações compartilhadas em rede, mas, diferentemente da *web* social, não se trata de *read-write*, mas de o que Naik e Shivalingaiah chamam de *read-write-execute*⁵⁰, ou seja, a

web 3.0 é a *web* onde o conceito de sítio da *internet* ou página da *internet* desaparece, onde dado não pertence a alguém, mas é compartilhado instantaneamente, onde os serviços mostram diferentes formas para o mesmo fim ou dado.⁵¹

A *web* semântica foi explorada por trilhões de usuários conectados em rede, com bilhões de dados compartilhados⁵². Segundo Keen⁵³, a *web* 3.0 caracteriza-se essencialmente pelo culto do social, ou era do grande exibicionismo, onde se alimenta a rede com dados pessoais dos próprios usuários, desafiando a proteção de dados pessoais dos indivíduos. Conforme Keen, a *web* semântica pode ser traduzida como um *software* inteligente que pode usar as informações constantes na rede para induzir as decisões futuras de seus usuários bem como suas intenções⁵⁴. E é aqui, exatamente nesse cenário, com a evolução de computadores e dispositivos conectados em rede, com o objetivo de induzir decisões humanas por *softwares* inteligentes, que se insere a confecção do conceito de *internet* das coisas.

Em que pese não haver um conceito único para IoT, Magrani a qualifica como sendo

um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de imputação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. O que todas as definições de IoT têm em comum é que elas se concentram em como

- Curso de Programa de Pós-graduação Stricto Sensu em Direito, Departamento de Ciências Sociais Aplicadas, Universidade Regional Integrada do Alto Uruguai e das Missões, Santo Ângelo, 2019. p. 29.

⁵⁰ Tradução livre de: "Web 3.0 is a web where the concept of website or webpage disappears, where data isn't owned but instead shared, where services show different views for the same web/the same data". NAIK, Umsha; SHIVALINGAIAH, D. Comparative Study of Web 1.0, Web 2.0 and Web 3.0. In: 6° INTERNATIONAL CALIBER, 6., 2008, Allahabad. **Anais 6° International CALIBER**. Allahabad: Inflibnet Centre, 2008. v. 1, p. 499-507. p. 501-502. Disponível em: <https://ir.inflibnet.ac.in/bitstream/1944/1285/1/54.pdf>. Acesso em: 22 abr. 2020.

⁵¹ NAIK, Umsha; SHIVALINGAIAH, D. Comparative Study of Web 1.0, Web 2.0 and Web 3.0. In: 6° INTERNATIONAL CALIBER, 6., 2008, Allahabad. **Anais 6° International CALIBER**. Allahabad: Inflibnet Centre, 2008. v. 1, p. 499-507. Disponível em: <https://ir.inflibnet.ac.in/bitstream/1944/1285/1/54.pdf>. Acesso em: 22 abr. 2020.

⁵² *Idem*.

⁵³ KEEN, Andrew. **The cult of the amateur**: how today's internet is killing our culture. Nova Iorque: Doubleday, 2007. p. 182.

⁵⁴ *Idem*.

computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade.⁵⁵

Fato é que, a partir do surgimento da humanidade, evoluiu consigo a necessidade de se salvaguardar, como um corolário da vida animal, a privacidade. Homens e animais, assim, buscaram ainda em tempos rudimentares estabelecer os limites do relacionamento social a fim de delimitar o que é de uso comum e o que é de uso compartilhado. Com o avanço do conceito de privacidade, os ordenamentos jurídicos ao redor do mundo passaram a tutelar a vida privada como um ramo do Direito Civil, inserindo em suas codificações a constitucionalidade do direito de personalidade. Tendo em vista que a vida privada passou a ser tutelada pelo Direito, a proteção de dados pessoais também mereceu guarida legislativa, razão pela qual, igualmente, incontáveis leis protetivas de dados pessoais passaram a ocupar espaço nos ordenamentos jurídicos dos Estados democráticos. O avanço da *internet*, por outro lado, fez com que a distribuição e o compartilhamento de dados, o que, portanto, pode assolar a privacidade, se propagasse, e, com a progressão do uso das novas tecnologias, a *internet* das coisas se mostrou como um novo desafio às legislações que se preocupam em proteger a privacidade e os dados pessoais.

A IoT, portanto, nada mais é do que a hiperconectividade de dispositivos entrelaçados com o fito de que, ligados à *internet*, executem tarefas de forma automatizada para criar facilidades no cotidiano das pessoas. Alcantara afirma que hiperconectividade significa “possibilitar, a qualquer tempo e lugar, a comunicação com qualquer coisa. É uma nova tendência e mais um passo muito importante do crescimento da tecnologia”⁵⁶. Ocorre que não são apenas os indivíduos que estão conectados, mas também as máquinas, uma vez que, para que a IoT opere, necessariamente deve haver a comunicação entre indivíduos e máquinas (*human-to-machine*, H2M, ao se ordenar um comando ao computador para que este se programe a executar uma tarefa) e entre máquinas com máquinas (*machine-to-machine*, M2M, ao entrelaçar dados e executar tarefas de forma automatizada e inteligente).

⁵⁵ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 20.

⁵⁶ ALCANTARA, Larissa Kakizaki de. **Big Data e Internet das Coisas: desafios da privacidade e da proteção de dados no Direito Digital**. São Paulo: Independente, 2017. p. 12.

Nesse sentido, Lemos e Bitencourt⁵⁷ chamam de sensibilidade performativa o que entendem ser “uma das características essenciais dos sistemas de IoT”⁵⁸. Parafraseando os autores, Lemos e Jesus dizem que

os novos objetos dotados de qualidade infocomunicacionais são sencientes e produzem, a partir de uma sensibilidade eletrônica, agências algorítmicas complexas em uma rede ampla. Assim, por exemplo, as lixeiras inteligentes de Dublin [...] podem saber quando estão cheias, avisar os poderes públicos, montar a rota de coleta e servir como instrumento de discursos sobre eficiência, melhoria da limpeza urbana e da qualidade de vida.⁵⁹

Portanto, a sensibilidade performativa corresponde à teia de objetos que se comunicam sem interação humana. Para Alcantara, são objetos conectados que se utilizam “da inteligência, da *internet*, gerando inúmeras possibilidades e oportunidades de negócios nos mais variados setores. O termo utilizado, inclusive, é *machine to machine* ou M2M”⁶⁰, ou seja, interação entre máquinas. Através da sensibilidade performativa, os dispositivos conectados em rede *on-line* podem trocar “informações e comandos entre si para que determinada ação seja executada”⁶¹. A expressão IoT “é utilizada para designar a conectividade e interação entre vários tipos de objetos do dia a dia, sensíveis à *internet*”⁶². Daí o termo *internet* associado ao termo das coisas, porque as coisas (objetos, itens, instrumentos etc.) que anteriormente eram analógicas, *off-lines*, hoje passam a compor o ciberespaço conectados à rede mundial de computadores.

A sigla IoT refere-se a um mundo onde coisas e seres humanos interagem uns com os outros durante todo o tempo e em qualquer espaço⁶³, e fora alcunhada por Kevin Ashton, do *Massachusetts Institute of Technology*, em 1999. De acordo com Ashton, em publicação ao *RFID Journal* em 2009, as pessoas necessitam

⁵⁷ LEMOS, André; BITENCOURT, Elias. Sensibilidade Performativa e Comunicação Das Coisas. **Matrizes**, São Paulo, v. 3, n. 12, p.165-188, set. 2018. Disponível em: <https://www.revistas.usp.br/matrizes/article/download/147528/149830/>. Acesso em: 08 jun. 2019.

⁵⁸ LEMOS, André; JESUS, Raniê Solarevisky de. Salvador, cidade inteligente? Comunicação e invisibilidade em experiências de IoT na capital baiana. **Revista Eco-pós**, [S.l.], v. 20, n. 3, p.66-92, 18 dez. 2017. Revista ECO-Pos. <http://dx.doi.org/10.29146/eco-pos.v20i3.14474>. p. 68.

⁵⁹ *Idem*.

⁶⁰ ALCANTARA, Larissa Kakizaki de. **Big Data e Internet das Coisas**: desafios da privacidade e da proteção de dados no Direito Digital. São Paulo: Independente, 2017. p. 12.

⁶¹ *Idem*.

⁶² MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 44.

⁶³ NASCIMENTO, Rodrigo. **O que, de fato, é internet das coisas e que revolução ela pode trazer?**: a resposta saberemos nos próximos anos, mas uma coisa é certa, uma nova revolução digital está prestes a acontecer. 2015. Disponível em: <https://computerworld.com.br/2015/03/12/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer/>. Acesso em: 08 jun. 2019.

estarem conectadas à *internet* das mais variadas formas, devido à falta de tempo para realizarem tarefas mais simples do dia-a-dia, o que é delegado aos aplicativos de *internet* das coisas⁶⁴. A IoT, quando criada, portanto, veio a ser um instrumento facilitador do cotidiano de seus usuários⁶⁵. Já, nas palavras de Lemos e Bittencourt, *internet* das coisas corresponde a uma teia, cujas amarras se fazem através da *internet*, aonde “objetos físicos e digitais são instrumentalizados com sensores e interligados com capacidade de comunicação por redes”⁶⁶.

Fato é que a *internet* das coisas transforma o modo com que se vive, trabalha e aprende, e a existência de aplicações conectadas através de transmissão de dados por IoT é o início de um ciclo de renovação tecnológica que se dispõe a auxiliar na otimização e automatização das mais variadas tarefas básicas do quotidiano. Essas tarefas vão desde benefícios oriundos da seara pública até mesmo em uma remodelagem das empresas privadas, podendo garantir mais eficiência na prestação de seus serviços. Nesse sentido, a conexão de dados, pessoas e coisas atrela-se em inúmeras possibilidades. Santos, ao analisar a *internet* das coisas como um desafio à privacidade, enumera a IoT em “*Smart Cities, Smart Environment, Smart Metering, Segurança & Emergências, retalho, logística, controlo industrial, Smart Agriculture, Smart Animal Farmin, domótica e eHealth*”⁶⁷.

Dessa forma, vários são os exemplos de aplicações conectadas à *internet* das coisas. Na área da saúde, as aplicações vinculadas à *internet* das coisas são conhecidas como *eHealth* e servem, basicamente, para “tentar controlar as doenças crónicas [sic], melhorar os diagnósticos, arranjar novas soluções de tratamento e, com isto, prolongar e melhorar a qualidade de vida da população”⁶⁸. É que, segundo Fornasier, a *internet* das coisas voltada a aplicações de saúde “tem potencial de

⁶⁴ ASHTON, Kevin. **That 'Internet of Things' Thing**. 2009. Disponível em: <https://www.rfidjournal.com/articles/view?4986>. Acesso em: 08 jun. 2019.

⁶⁵ *Idem*.

⁶⁶ LEMOS, André; BITENCOURT, Elias. Sensibilidade Performativa e Comunicação Das Coisas. **Matrizes**, São Paulo, v. 3, n. 12, p.165-188, set. 2018. Disponível em: <https://www.revistas.usp.br/matrizes/article/download/147528/149830/>. Acesso em: 08 jun. 2019. p. 166.

⁶⁷ SANTOS, Pedro Miguel Pereira. **Internet das coisas: o desafio da privacidade**. 2016. 108 f. Dissertação (Mestrado) - Curso de Sistemas de Informação Organizadas, Instituto Politécnico de Setúbal, Setúbal, 2016. Disponível em: <http://comum.rcaap.pt/bitstream/10400.26/17545/1/Disserta%c3%a7%c3%a3o%20Pedro%20Santos%20140313004%20MSIO.pdf>. Acesso em: 01 maio 2020. p. 11.

⁶⁸ MARTINS, Joana Castel-Branco Saldanha. **A Internet das Coisas em Serviços de Saúde**. 137 f. Dissertação (Mestrado) – Faculdade de Economia e Gestão, Universidade Católica Portuguesa, Porto, 2019. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/28405/1/TFM_JoanaSaldanha.pdf. Acesso em: 17 abr. 2021. p. 39.

reduzir dias e internações hospitalares através da utilização de *wearables*, que permitem um monitoramento durante 24 horas e 7 dias por semana aos pacientes”⁶⁹. Para o autor, as principais alternativas de conectividade capazes de trazer maior controle autônomo da saúde do usuário são os *wearables* (vestíveis ligados ao corpo humano que capturam dados) e os *smartphones* (celulares inteligentes que interpretam os dados capturados pelos *wearables*)⁷⁰, mas, para além destes, há uma série de soluções criadas para a *eHealth*. Exemplos são o ambiente assistido, uma extensão para vida independente de indivíduos idosos com um gerenciamento seguro, dando assistência humana em caso de algum problema ocorrer; a *internet* das coisas médicas e de saúde, ou seja, computadores, sensores médicos e tecnologias de comunicação para serviços de cuidado de saúde; e o aviso de uso de medicamento, onde o próprio paciente pode identificar, através de seu dispositivo de IoT, qual droga precisa consumir naquele momento⁷¹.

Assim, a utilização de IoT para aprimoramento e indução de um maior cuidado com a saúde do usuário nada mais é do que se valer de dispositivos que possam monitorar o corpo humano e, em caso de algum potencial dano à saúde, alertem a busca da medicina especializada ou mesmo, em casos como o do ambiente assistido, prontamente acionem, independentemente de ação humana, cuidados emergenciais de sobreaviso. Nesse sentido, a *internet* das coisas tem o potencial de revolucionar a forma como se desenvolvem os sistemas de cuidado com a saúde humana – e o próprio cuidado por si só –, através da implementação de técnicas e dispositivos que, dotados de inteligência artificial, *machine learning* e *big data*, são capazes de fazer melhores diagnósticos, prognósticos, prevenções e tratamentos.

É por isso que, desde as aplicações de saúde até cafeteiras que programam o café sozinhas, passando por casas inteligentes auxiliadas por dispositivos como *Alexa* e *Google Home*, a *internet* das coisas é um grande emaranhado de encantadores apoiadores à vida humana. Conforme Lemos e Jesus, os projetos de

⁶⁹ Tradução livre de: “IoMT has potential to reduce days and admissions in healthcare institutions due to the mobility of the wearables, wich allow 24/7 monitoring of patients”. FORNASIER, Mateus de Oliveira. The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy. **Rev. Investig. Const.**, Curitiba, v. 6, n. 2, p.297-321, maio 2018. Disponível em: <https://revistas.ufpr.br/rinc/article/view/67592/39878>. Acesso em: 17 abr. 2021. p. 302.

⁷⁰ *Idem.*

⁷¹ *Idem.*

smart cities, por sua vez, “atestam o conceito de IoT proposto por Ashton”⁷², uma vez que se valem – as *smart cities* – de inúmeras iniciativas que, conectadas à sensores ligados à *internet*, formam uma grande base de dados hábil a promover serviços públicos de forma autônoma, inteligente e útil. As *smart cities*, atualmente, são projetos cobiçados em vários países, porque, na concepção dos autores, traz à tona um discurso ideológico de “promoção do uso de tecnologias de informação e comunicação por empresas e governos para melhorar a gestão das cidades e a vida dos cidadãos”⁷³, e a região que concentra o maior número de aplicações de *smart cities* no mundo é os Estados Unidos, seguida pela Europa, Ásia e Oceania⁷⁴.

No Brasil, o grande exemplo de projeto de implementação de IoT para a construção de uma *smart city* está ilustrado na cidade de Salvador, no estado da Bahia. A capital baiana é a terceira maior cidade do Brasil em número de habitantes, razão pela qual foi necessária a implementação de IoT para a efficientização do município. Desta maneira, em Salvador, alguns processos de *internet* das coisas, através da conexão de sensores inteligentes à rede mundial de computadores, foram implementados: “instalação de sistemas de automação e monitoramento no trânsito, nas atividades da defesa civil, nas redes de distribuição de energia elétrica e na mensuração dos índices de qualidade do ar”⁷⁵. Também, a implementação da *internet* das coisas na capital baiana fez com que os semáforos da cidade se tornassem inteligentes. Explica-se: a Transalvador, empresa que administra o trânsito na cidade, implantou 340 (trezentos e quarenta) câmeras espalhadas pela capital. Dessa forma, vigiando as rotas de Salvador, o sistema pode rastrear a posição dos veículos, uma vez que o automóvel cruze o sensor instalado abaixo da câmera de vigilância. A consequência disso é que “o movimento dos carros é captado pela controladora [...], que aciona os semáforos nas cercanias para garantir um fluxo contínuo”⁷⁶.

Se não bastasse isso, a maior fluidez do trânsito baiano, um dos grandes problemas das grandes cidades atualmente, fora confeccionado o Centro de

⁷² LEMOS, André; JESUS, Raniê Solarevisky de. Salvador, cidade inteligente? Comunicação e invisibilidade em experiências de IoT na capital baiana. **Revista Eco-pós**, [S.l.], v. 20, n. 3, p.66-92, 18 dez. 2017. Revista ECO-Pos. <http://dx.doi.org/10.29146/eco-pos.v20i3.14474>. p. 68.

⁷³ *Ibidem*. p. 69.

⁷⁴ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 85.

⁷⁵ LEMOS, André; JESUS, Raniê Solarevisky de. Salvador, cidade inteligente? Comunicação e invisibilidade em experiências de IoT na capital baiana. **Revista Eco-pós**, [S.l.], v. 20, n. 3, p.66-92, 18 dez. 2017. Revista ECO-Pos. <http://dx.doi.org/10.29146/eco-pos.v20i3.14474>. p. 69.

⁷⁶ *Idem*.

Monitoramento e Alarme da Defesa Civil, também na capital da Bahia. Dita central visa cuidar do sistema de monitoramento de deslizamento de encostas em áreas vulneráveis na cidade. Através do CEMADEC, fora criada uma estação totalmente robotizada, posicionada de frente para as encostas, que “dispara raios infravermelhos em cada um dos prismas calculando se houve alguma alteração na posição dos espelhos”⁷⁷, realizando “completa varredura do conjunto de prismas a cada 25 minutos”⁷⁸. O curioso é que o sistema implementado não aciona, segundo Jesus e Lemos, sirene alguma, para não alarmar a população que vive na encosta, e que, uma vez que se detectam oscilações geográficas através de raios infravermelhos, há tempo suficiente para que a Defesa Civil se desloque e possa porventura evitar grandes tragédias aos habitantes daquelas localidades⁷⁹. Nesse sentido, Magrani diz que o

poder público demonstra já estar atento aos benefícios da IoT, entendendo que esta surge como importante ferramenta voltada para os desafios da gestão pública, prometendo, a partir do uso de tecnologias integradas e do processamento massivo de dados, soluções mais eficazes para problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros.⁸⁰

Portanto, a *internet* das coisas surgiu, quando englobada na administração pública, como um grande instrumento facilitador para governos melhorarem a gestão das cidades e a vida de seus cidadãos. Ocorre que não é somente em escala estatal que a IoT opera, e, sim, também em proporções privadas. Exemplo disto é a sua utilização por empresas. Magrani⁸¹ diz que, quando as coisas estão conectadas à *web*, há como se oferecer dados sobre o uso daquela coisa específica, razão pela qual o tratamento de informação sobre o uso efetivo pelos clientes-alvo dos produtos e serviços da empresa é capaz de oferecer novos modelos de negócios, serviços e produtos úteis às necessidades dos clientes.

Quanto às pessoas, a IoT também vem buscando sua inserção às necessidades individuais. Exemplo disso são os carros inteligentes. No setor automotivo, recentemente a Tesla Inc., uma das montadoras de automóveis mais

⁷⁷ LEMOS, André; JESUS, Raniê Solarevisky de. Salvador, cidade inteligente? Comunicação e invisibilidade em experiências de IoT na capital baiana. **Revista Eco-pós**, [S.l.], v. 20, n. 3, p.66-92, 18 dez. 2017. Revista ECO-Pos. <http://dx.doi.org/10.29146/eco-pos.v20i3.14474>. p. 75.

⁷⁸ *Idem*.

⁷⁹ *Idem*.

⁸⁰ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 81-82.

⁸¹ *Ibidem*. p. 81.

tecnológicas do mundo e dentre as primeiras a alocar veículos eco sustentáveis movidos à energia elétrica, acoplou a IoT em seus protótipos. Brisbane diz que, por meio da *internet* das coisas, é possível que se conecte os veículos aos *smartphones* que a eles estão pareados, a fim de que se verifique, pelo aparelho celular, o nível de bateria do automóvel, bem como sua localização via sistema de monitoramento GPS, o controle de sua temperatura interna e outras funcionalidades⁸². O objetivo dessas inovações, segundo Brisbane, é evitar que o conforto excessivo da temperatura, por exemplo, acarrete em ligeiro relaxamento e consequente desatenção do motorista ao volante⁸³, evitando, assim, eventuais acidentes de trânsito.

Nessa mesma linha, especificamente quanto às aplicações de IoT voltadas à saúde de seu usuário, Santos afirma que alguns dos ícones atuais de aplicações conectadas à *internet* das coisas são os *wearables* e os *portables*⁸⁴. Trata-se daqueles dispositivos que, ligados ao corpo humano, são capazes de medir dados como qualidade do sono, hora de comer, nível de atividade física e batimentos cardíacos, sedentarismo etc. Santos lembra que os “*wearables* têm sido altamente utilizados como uma tecnologia inovadora na área da saúde, pela sua capacidade em registrar continuamente as estatísticas vitais e observações em tempo real, como a pressão arterial, remotamente”⁸⁵. Quando o assunto é *eHealth*, exemplos de IoT são os *wearables* e *portables*, os *Smart Watches*, as *Smart Bands*, os *Smart Glasses*, os *Fitness Trackers* etc. Os *wearables* são vestíveis, isto é, apetrechos que envolvam tecnologia e que o usuário possa vestir, usar como acessório, carregar consigo da maneira que bem entender. Já os *portables* são os *softwares*, isto é, as instalações contidas dentro dos *wearables*, o que transforma um simples relógio em um *smartwatch*, por exemplo. E o que torna realmente interessante a utilização deste tipo de aplicação é a possibilidade de “monitorar as condições de um paciente e notificar familiares, prestadores de cuidados médicos ou serviços de emergência

⁸² BRISBOURN, Alex. **Tesla's Over-the-Air Fix**: best example yet of the internet of things?. Disponível em: <https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/>. Acesso em: 15 jun. 2019.

⁸³ *Idem*.

⁸⁴ SANTOS, Pedro Miguel Pereira. **Internet das coisas**: o desafio da privacidade. 2016. 108 f. Dissertação (Mestrado) - Curso de Sistemas de Informação Organizadas, Instituto Politécnico de Setúbal, Setúbal, 2016. Disponível em: <http://comum.rcaap.pt/bitstream/10400.26/17545/1/Disserta%20a7%20a3o%20Pedro%20Santos%20140313004%20MSIO.pdf>. Acesso em: 01 maio 2020. p. 14.

⁸⁵ *Idem*.

conectados ao sistema de incidentes de riscos potenciais, como quedas, mudanças de dieta, ou mudanças de temperatura”⁸⁶.

Acontece que os avanços da *internet* das coisas na saúde não param por aí. Recente estudo publicado pelo grupo de telemedicina Morsch dá conta de que o uso da *internet* das coisas na *eHealth* pulverizou-se em nove novos ramos que, antes da evolução da rede, não se cogitava. Para os médicos, a IoT é capaz de garantir registros digitais de exames “capazes de gerar e armazenar dados digitais, eliminando o uso de papel”⁸⁷. Entendem os pesquisadores que isso faz com que, além de se preservar o meio ambiente e garantir maior sustentabilidade ao sistema de saúde, se reduza o espaço físico de arquivos, permitindo maior simplicidade no compartilhamento de informações:

Atualmente, existem aparelhos digitais para exames de diagnóstico – como raio X, tomografia e eletrocardiograma -, capazes de gerar e armazenar dados digitalmente, eliminando o uso de papel. Essa possibilidade preserva o meio ambiente, reduz a necessidade por espaço físico para arquivos e garante a conservação dos documentos, sem qualquer cuidado adicional como no manuseio de filmes radiográficos, que poderiam ser facilmente danificados. Arquivadas digitalmente, as informações permitem maior simplicidade no compartilhamento, que pode ser feito via e-mail ou aplicativos de mensagens.⁸⁸

A digitalização de arquivos em exames digitais, que são diagnosticados diretamente a partir das aplicações vinculadas à IoT, tem condão de dinamizar o acesso dos pacientes ao resultado da investigação médica realizada. Também, faz com que menos circulação haja nos laboratórios, fluindo a operacionalização do serviço exclusivamente para a realização de novos procedimentos, e não para a conferência de exames já realizados.

Morsch ainda saúda a utilização de marca-passos cardíacos com dispositivos de IoT, o que, por si só, uma vez que implantados nos pacientes, “facilitam o

⁸⁶ SANTOS, Pedro Miguel Pereira. **Internet das coisas**: o desafio da privacidade. 2016. 108 f. Dissertação (Mestrado) - Curso de Sistemas de Informação Organizadas, Instituto Politécnico de Setúbal, Setúbal, 2016. Disponível em: <http://comum.rcaap.pt/bitstream/10400.26/17545/1/Disserta%c3%a7%c3%a3o%20Pedro%20Santos%20140313004%20MSIO.pdf>. Acesso em: 01 maio 2020. p. 11.

⁸⁷ MORCH. **IoT na Medicina**: 9 Exemplos de como a Internet das Coisas avança na saúde. 29 abr. 2019. Disponível em: <https://telemedicinamorsch.com.br/blog/iot-na-medicina>. Acesso em: 17 dez. 2020.

⁸⁸ *Idem*.

acompanhamento cardiovascular de milhares de pessoas nos Estados Unidos”⁸⁹. Para os médicos, tal qual aos *warables* e *portables* anteriormente narrados (os *Smart Watches*, as *Smart Bands*, os *Smart Glasses*, e os *Fitness Trackers*, por exemplo), os marca-passos inteligentes são capazes de armazenar dados importantes, em tempo real, sobre o sistema cardíaco do paciente, compartilhando-os imediatamente com as clínicas médicas contratadas:

Alguns aparelhos conectados podem ser implantados no paciente. É o caso de marcapassos inteligentes, que facilitam o acompanhamento de milhares de pessoas nos Estados Unidos. Assim como os wearables, esses dispositivos coletam, armazenam e enviam informações em tempo real sobre o sistema cardiovascular do paciente. Dessa forma, o cardiologista e outros profissionais podem monitorar as condições de saúde do indivíduo à distância, intervindo quando necessário.⁹⁰

É através do compartilhamento dos dados cardiovasculares, em tempo real, que a *internet* das coisas se mostra como uma importante ferramenta para a prevenção de doenças cardíacas que, se não tratadas em tempo hábil, poderiam se apresentar como fatais. Segundo a Morsch, “o cardiologista e outros profissionais podem monitorar as condições de saúde do indivíduo à distância, intervindo quando necessário”⁹¹, mas, para Fornasier, “o próprio paciente também pode tomar decisões para melhorar sua qualidade de vida”⁹² a partir das denúncias de estado clínico de saúde feitas pelos aparelhos conectados à IoT.

Recente investigação realizada pela Universidade Federal Tecnológica do Paraná criou uma proposta de protocolo de tele monitoramento sob a demanda de sinais biomédicos utilizando a *internet* das coisas, a computação móvel e o armazenamento em nuvem. O objetivo da pesquisa era desenvolver um sistema para a visualização de sinais bioelétricos, através de aplicações de marca-passos inteligentes, conectados à *internet* das coisas, por meio de armazenamento em

⁸⁹ MORCH. **IoT na Medicina**: 9 Exemplos de como a Internet das Coisas avança na saúde. 29 abr. 2019. Disponível em: <https://telemedicinamorsch.com.br/blog/iot-na-medicina>. Acesso em: 17 dez. 2020.

⁹⁰ *Idem*.

⁹¹ *Idem*.

⁹² Tradução livre de: “The patient would have, then, the opportunity to take care of herself/himself and play a more active role in the care process”. FORNASIER, Mateus de Oliveira. The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy. **Rev. Investig. Const.**, Curitiba, v. 6, n. 2, p.297-321, maio 2018. Disponível em: <https://revistas.ufpr.br/rinc/article/view/67592/39878>. Acesso em: 17 abr. 2021. p. 302..

nuvem⁹³. A investigação dividiu a tecnologia para a *internet* das coisas em três fases: coleta, transmissão, e gerenciamento e utilização de dados.

A primeira fase, da coleta, diz com o sensoriamento do ambiente físico, isto é, a captação de dados, em tempo real, provenientes dos sensores alocados ao corpo humano, capazes de medir temperatura, glicose, luminosidade, peso, batimentos cardíacos, frequência cardíaca etc. Esses dados, quando reconhecidos pela *internet* das coisas, são imediatamente comunicados a *wireless sensor networks*, ou seja, redes de sensoriamento remotas, destinadas a proceder pela transmissão dos dados. Nessa primeira etapa, os marca-passos inteligentes capturam os batimentos e a frequência cardíaca do coração a que estão acoplados. É aí que entra em vigência segunda fase da IoT em saúde: a transmissibilidade dos dados.

Segundo os investigadores, depois “disponibilizam os dados coletados para as aplicações que as demandem, é necessário transmitir estes dados para algum lugar ou servidor que as armazene para que outros aplicativos possam fazer uso de toda uma base”⁹⁴ de informação. Essa transmissibilidade de dados é feita, via de regra, através de redes sem fio de *internet*, mais precisamente aquelas que operam desde frequências de 2,4 GHz até frequências de 5 GHz⁹⁵. No Brasil, recentemente foram lançadas as primeiras experiências de conectividade 5G, embora o serviço ainda seja limitado⁹⁶. É de se ressaltar, por outro lado, um ponto de muita desconfiança sobre a conectividade 5G: em que pese o sinal estar disponível no Brasil, por exemplo, “só tem, atualmente, um aparelho de celular que suporta o 5G. Além disso, o sinal só vai ser ativado em alguns bairros de oito capitais do país”⁹⁷. Assim, ainda que consiga operar em redes de 2,4 a 4 GHz, a funcionalidade da IoT na saúde para redes de 5G, sua melhor velocidade, não será uma realidade em todo o território nacional nem a todos os seus usuários.

⁹³ MACHADO, Francisco Muller. **Proposta de protocolo de telemonitoramento sob demanda de sinais biomédicos usando internet das coisas, computação móvel e armazenamento em nuvem**. 2016. 132 f. Dissertação (Mestrado) – Programa de Pós-graduação em Engenharia Biomédica, Curitiba, 2016. Disponível em: <http://repositorio.utfpr.edu.br:8080/jspui/handle/1/1825>. Acesso em: 17 dez. 2020. p. 21.

⁹⁴ *Ibidem*. p. 69.

⁹⁵ *Ibidem*. p. 71.

⁹⁶ G1. **Operadoras lançam primeira experiência do 5G no Brasil, mas serviço ainda é limitado**. 29 jul. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/07/18/operadoras-lancam-primeira-experiencia-do-5g-no-brasil-mas-servico-ainda-e-limitado.ghtml>. Acesso em: 17 dez. 2020.

⁹⁷ *Idem*.

Por sua vez, a última etapa da proposta de protocolo de tele monitoramento sob a demanda de sinais biomédicos utilizando *internet* das coisas, computação móvel e armazenamento em nuvem toca sobre a fase de gerenciamento e utilização de dados. Conforme Machado,

esta fase é responsável por toda uma abstração das características dos objetos sensorados e posteriormente transmitidos, podendo também fornecer uma retroalimentação de controle aos aplicativos que fornecem os dados. Tudo que se relacione ao tratamento dos dados, desde análise semântica, filtragem ou outro tipo de tratamento que se faça necessário aos dados é aqui tratado.⁹⁸

Essa última fase destina-se justamente a realizar o tratamento dos dados primeiramente captados e posteriormente transmitidos ao banco de armazenamento. O tratamento de dados diz com a lapidação do dado em estado bruto, decodificando-o para que se torne possível sua leitura e interpretação por um operador. É justamente nessa fase, a de tratamento, que o marca-passos inteligente torna factível ao médico, ou mesmo ao próprio paciente, tomar conhecimento da real e imediata situação clínica cardiovascular do usuário de marca-passos conectado à *internet* das coisas, fazendo com que, segundo Morsch, de fato, se possa tomar “decisões para melhorar sua qualidade de vida”⁹⁹.

Outro item de telemedicina conectado à IoT é justamente o monitoramento contínuo inteligente de glicose. Essas aplicações são denominadas *continuous glucose monitor* (CGM), ou, em tradução livre, monitor contínuo de glicose, e são capazes de analisar e enviar dados de glicose a outro aparelho previamente cadastrado. Esses dispositivos surgiram, primordialmente, nos Estados Unidos, ainda nos anos 90, mas o primeiro CGM foi aprovado pela *Food and Drug Administration*, agência norte-americana que regula o uso de alimentos e medicamentos no país, somente em 1999¹⁰⁰, todavia sem habilidade para o compartilhamento dos dados captados. O uso dos CGMs, hoje em dia, é bastante importante, porque, na medida em que monitoram os níveis de glicose de diabéticos,

⁹⁸ MACHADO, Francisco Muller. **Proposta de protocolo de telemonitoramento sob demanda de sinais biomédicos usando internet das coisas, computação móvel e armazenamento em nuvem**. 2016. 132 f. Dissertação (Mestrado) – Programa de Pós-graduação em Engenharia Biomédica, Curitiba, 2016. Disponível em: <http://repositorio.utfpr.edu.br:8080/jspui/handle/1/1825>. Acesso em: 17 dez. 2020. p. 71.

⁹⁹ MORCH. **IoT na Medicina: 9 Exemplos de como a Internet das Coisas avança na saúde**. 29 abr. 2019. Disponível em: <https://telemedicinamorsch.com.br/blog/iot-na-medicina>. Acesso em: 17 dez. 2020.

¹⁰⁰ *Idem*.

por exemplo, podem calcular padrões que, se alterados, denunciam com brevidade anormalidades ainda contornáveis. A *internet* das coisas na saúde, através dos monitores contínuos de glicose, faz com que o diabetes, doença grave que necessita de acompanhamento diário, seja controlado através de dados precisos e instantâneos.

Também, exames de imagem hoje em dia podem ser substituídos por aplicações conectadas à *internet* das coisas. Assim acontece com a colonoscopia, procedimento em que uma câmera é inserida no investigado a fim de captar imagens de seu sistema digestivo. A colonoscopia costuma ser um exame extremamente desconfortável aos pacientes, razão pela qual a empresa *Given Imaging*, sediada na Geórgia, nos Estados Unidos, criou a *PillCam Colon*¹⁰¹. Essa nova câmera nada mais é do que uma pílula, do tamanho de um suplemento vitamínico, ingerida pelo paciente com água. Essa pílula filmadora realiza o procedimento colonoscópico, sem a necessidade de o investigado submeter-se ao exame tradicional. Mais um exemplo importante são as *Scripps Healths*, nano sensores que, quando ingeridos, vão à corrente sanguínea, local de onde enviam informações sobre o sistema cardiovascular do paciente ao sistema de saúde¹⁰².

Interessante mecanismo relatado pela farmacêutica Takeda foi a utilização de *wearables*, como *Smart Watches*, para aplicação de testes em pacientes diagnosticados com transtornos depressivos leves e moderados. Utilizou-se, assim, da *internet* das coisas para monitorar o comportamento dessas pessoas com depressão. O estudo apontou que “as avaliações de humor e cognição tiveram mais de 90% de eficácia, enquanto avaliações diárias feitas a partir de questionários e outros dados corresponderam aos resultados de testes”¹⁰³ com considerável menor grau de efetividade. O objetivo do estudo era comparar a participação de pacientes em testes tecnológicos com a participação em testes tradicionais, o que acabou por

¹⁰¹ GIVEN IMAGING. **Cápsula endoscópica para endoscopia digestiva**. Disponível em: <https://www.medicalexpo.com/pt/prod/given-imaging/product-75056-720465.html>. Acesso em 17 dez. 2020.

¹⁰² FORBES. **How IoT is changing the Science of medicine**. Disponível em: <https://www.forbes.com/sites/insights-inteliot/2018/09/14/how-iot-is-changing-the-science-of-medicine/?sh=2e4a79f33e57>. Acesso em 17 dez. 2020.

¹⁰³ MORCH. **IoT na Medicina: 9 Exemplos de como a Internet das Coisas avança na saúde**. 29 abr. 2019. Disponível em: <https://telemedicinamorsch.com.br/blog/iot-na-medicina>. Acesso em: 17 dez. 2020.

certificar que “participantes que estavam realizando testes através de *Apple Watch* tinham por hábito a realização diária da avaliação de humor”¹⁰⁴.

Casuístico exemplo é da própria IBM, gigante *player* estadunidense da indústria de tecnologia, que, em parceria com a farmacêutica norte-americana Pfizer, desenvolveu um sistema de monitoramento da doença Mal de Parkinson através de sensores e análises que mapeiam e buscam melhorar os ensaios clínicos dos pacientes. Essa parceria foi batizada de *BlueSky Project*, ou, em tradução livre, Projeto Céu Azul, cujo objetivo era desenvolver um sistema para captar “passivamente dados de pessoas com doença de Parkinson continuamente em sua vida diária. Essa coleta de dados forneceria uma estimativa em tempo real de sua função motora, que é análoga aos escores obtidos durante um exame”¹⁰⁵ neurológico padrão.

O último caso é o dos *Smart Hospitals*. Segundo Martins, “60% das organizações de saúde no mundo já tinham introduzido *IoT devices* nas suas infraestruturas”¹⁰⁶. Atualmente, os hospitais inteligentes, tradução livre de *smart hospitals*, são aqueles que não mais dependem de papel, tornando-se *paperless*, e dependentes de “*devices* conectados e sensores para captar, traduzir e guardar informação crucial”¹⁰⁷. O objetivo dos hospitais inteligentes, na contramão dos grandes riscos a que estão expostos, como invasões feitas a seus bancos de dados e sistemas, é melhorar o diagnóstico dos pacientes, através da criação de novos métodos de tratamento e da melhoria daqueles já existentes, melhorar o fluxo de pacientes, dar assistência médica remota e aumentar a segurança do paciente, atuando na prevenção e doenças.

¹⁰⁴ Tradução livre de: “Participants were provided with an Apple Watch on which cognitive and mood tests were administered daily”. CISION PR NEWSWIRE. **Takeda and cognition kit presente results from digital wearable technology study in patients with major depressive disorder**. Disponível em: <https://www.prnewswire.com/news-releases/takeda-and-cognition-kit-present-results-from-digital-wearable-technology-study-in-patients-with-major-depressive-disorder-mdd-300558846.html>. Acesso em 17 dez. 2020.

¹⁰⁵ Tradução livre de: “The goal of the BlueSky project is to develop a system to passively capture data from people with PD continuously in their daily life. This data collection would provide a real-time estimate of their motor function that is analogous to scores obtained during a standard neurological exam”. IBM. **Monitoring Parkinson’s disease with sensors and analytics to improve clinical trials**. 11 abr. 2017. Disponível em: <https://www.ibm.com/blogs/research/2017/04/monitoring-parkinsons-disease/>. Acesso em 17 dez. 2020.

¹⁰⁶ MARTINS, Joana Castel-Branco Saldanha. **A internet das coisas em serviços de saúde**. 2019. 137 f. Dissertação (Mestrado) – Universidade Católica Portuguesa, Portugal, 2019. Disponível em: <https://repositorio.ucp.pt/handle/10400.14/28405>. Acesso em: 17 dez. 2020. p. 44.

¹⁰⁷ *Idem*.

Esses exemplos demonstram como a *internet* das coisas pode ser enfrentada como um fenômeno hábil a trazer maior conforto a seus usuários. Fato é que se trata de inegável avanço tecnológico, inovação que fora criada para auxiliar aqueles que a utilizam. Através da IoT, como se pode demonstrar, a administração pública consegue eficientizar a prestação de seu serviço, por meio da implementação de cidades inteligentes – *smart cities* –, retificando eventuais problemas de trânsito e evitando catástrofes ambientais. Na iniciativa privada, por sua vez, a conexão de dispositivos à rede é capaz de destacar quais são as reais necessidades dos consumidores, a fim de que se aperfeiçoe a prestação de serviço e a criação de produtos pelas empresas. Já no âmbito individual, os carros inteligentes, a exemplo da Tesla Inc., podem garantir maior segurança e conforto a seus motoristas e passageiros, porque automatiza a tomada de algumas decisões, como o condicionamento da temperatura interna do veículo, evitando que um conforto excessivo gere algum ligeiro relaxamento e conseqüente desatenção ao eventual motorista.

Contudo, segundo apontado por Magrani, Jarmoc salienta¹⁰⁸ que “a *internet* foi projetada para resistir a uma explosão nuclear. Mas não a um ataque de torradeiras”¹⁰⁹. E a colocação de Jarmoc se justifica porque os objetos conectados em rede, sob o manto da *internet* das coisas, em que pese facilitarem a vida de seus usuários, possuem seu lado perverso. É o caso da catalogação e do tratamento de dados pessoais oriundos de suas aplicações. Lemos e Bittencourt, nesse sentido, sustentam que os objetos conectados em rede, através de inteligência artificial, “sentem o mundo, produzem dados e agem de forma autônoma e independente de uma intervenção humana direta”¹¹⁰. E esse modo perspicaz de sentir o mundo, de comunicar entre si e de agir independentemente de ordem ou ingerência humana é o que caracteriza o conceito de *internet* das coisas.

Em razão da sensibilidade performativa associada aos objetos conectados pela rede, Greenfield denuncia que a *internet* das coisas “está próxima ao corpo [daquele que está utilizando um dispositivo identificado como IoT], onde pode medir

¹⁰⁸ JARMOC, Jeff. **In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters**. 21 out. 2016. Twitter: @jjarmoc. Disponível em: <https://twitter.com/jjarmoc/status/789637654711267328>. Acesso em: 25 abr. 2020.

¹⁰⁹ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 31.

¹¹⁰ LEMOS, André; BITENCOURT, Elias. Sensibilidade Performativa e Comunicação Das Coisas. **Matrizes**, São Paulo, v. 3, n. 12, p.165-188, set. 2018. Disponível em: <https://www.revistas.usp.br/matrizes/article/download/147528/149830/>. Acesso em: 08 jun. 2019. p. 166.

informações individuais como identidade, localização e saúde”¹¹¹. Lemos e Bittencourt, no mesmo sentido, dizem que a sensibilidade performativa

ultrapassa a simples comunicação de índices biométricos (temperatura, pressão arterial, glicemia etc.), de informações sobre incidência UV ou nível de CO₂ nas ruas, ampliação de sinal sonoro (aparelhos de ouvido) ou compensação de frequências cardíacas (marca-passo), comuns aos processos rudimentares de automação. [...], a SP da IoT não se restringe à captação ou mera apresentação de indicadores, mas, como veremos, constrói narrativas, sugere ações e produz perfis a partir dos dados extraídos.¹¹²

Em recente investigação realizada pela Universidade do Vale do Rio dos Sinos, Oliveira, Gomes, Lopes e Nobre dizem serem “grandes os desafios do tema proposto [privacidade na IoT] devido a complexibilidade de aplicar requisitos de segurança a objetos com processamento, memória, largura de banda e energia restritos”¹¹³. Isso porque, para os pesquisadores, a forma de armazenamento e segurança dos dados dos usuários das aplicações está diretamente relacionada à maneira como os dados serão protegidos. Os autores entendem que, uma vez que depositados em redes de compartilhamento *on-line*, impacta-se os protocolos de segurança, fazendo com que, a cada transmissão de dados, estes possam ser perdidos e vazados da rede¹¹⁴.

Para ilustrar a importância da proteção aos dados pessoais, especialmente aqueles oriundos de aplicações relacionadas à *internet* das coisas, recorda-se do caso *Yahoo*¹¹⁵. Na primavera de 2016 revelou-se que o *Yahoo*, uma das maiores empresas de tecnologia do mundo, com seu ramo de atuação amplamente concentrado na rede mundial de computadores, revelou invasão sofrida em seu

¹¹¹ Tradução livre de: “Tabs, being the smallest, were also the most personal; they stayed close to the body, where they might mediate individual information such as identity, location and availability”. GREENFIELD, Adam. **Everyware**: the dawning age of ubiquitous computing. Berkeley: New Riders, 2006. p. 14.

¹¹² LEMOS, André; BITENCOURT, Elias. Sensibilidade Performativa e Comunicação Das Coisas. **Matrizes**, São Paulo, v. 3, n. 12, p.165-188, set. 2018. Disponível em: <https://www.revistas.usp.br/matrizes/article/download/147528/149830/>. Acesso em: 08 jun. 2019. p. 166.

¹¹³ OLIVEIRA, Nairobi Spiecker de; GOMES, Moises Alexandre; LOPES, Ronaldo; NOBRE, Jeferson C.. Segurança da Informação para Internet das Coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD). **Revista Eletrônica de Iniciação Científica em Computação**, Porto Alegre, v. 17, n. 4, p. 1-14, jun. 2019. Disponível em: <https://www.seer.ufrgs.br/reic/article/view/88790/55009>. Acesso em: 01 maio 2020. p. 13.

¹¹⁴ *Ibidem*. p. 10-11.

¹¹⁵ HIGA, Paulo. **De novo**: Yahoo admite outro vazamento, agora com 1 bilhão de contas afetadas. Yahoo admite outro vazamento, agora com 1 bilhão de contas afetadas. 2016. Disponível em: <https://tecnoblog.net/204918/yahoo-vazamento-1-bilhao/>. Acesso em: 25 abr. 2020.

banco de dados que acarretou na exposição de aproximadamente 1 bilhão de usuários. O ataque sofrido pela empresa direcionou-se aos nomes, endereços, e-mail e mesmo dados de cartão de crédito daqueles que possuíam cadastro atualizado junto à empresa. E, se não bastasse, os invasores instalaram, à época, cookies para ter acesso a dados futuros destes usuários¹¹⁶. Isso quer dizer que mesmo aqueles que, à época da ação, não possuíam dados vinculados ao *Yahoo*, no momento em que utilizassem alguma das aplicações fornecidas pela programadora estariam sujeitos a terem seus dados pessoais vazados. E, mesmo tendo o *Yahoo* revelado no final de 2016 o vazamento, é importante salientar que a invasão ao seu banco de dados se deu ainda no ano de 2013, isto é, três anos antes que os usuários, titulares dos dados pessoais violados, dessem conta.

Outro importante caso ocorreu junto ao *Google*¹¹⁷, mais um gigante da internet. O *Google* é detentor de inúmeras aplicações envolvendo a internet das coisas. Um de seus mais relevantes aplicativos, neste segmento, é o *Google Home*, instrumento destinado a realizar a automatização da residência do usuário através de inteligência artificial. E o *Google Home*, assim como as demais aplicações pertencentes ao *Google*, vincula-se à conta pessoal do usuário titular de dados. Todos os dados dos usuários de aplicativos pertencentes ao *Google* estão armazenados na mesma conta. Através da instrumentalização do *Google Home*, um robô que vê, sente e fala, o *Google* armazena diariamente incontáveis bytes de dados domésticos e vitais dos usuários de seus serviços. Surpreendentemente, entretanto, mesmo diante de tantos dados pessoais, em 2018 o *Google* sofreu importante caso de vazamento e dados em uma de suas redes sociais, o *Google+*. Consequentemente, mais de 50 milhões de contas, desde pessoas físicas até perfis corporativos, tiveram seus dados expostos na rede mundial de computadores. Isso fez com que o *Google*, em agosto de 2019, desse fim àquela rede social.

Mas o que se faz com o tratamento de dados pessoais capturados através da internet das coisas? Pasquale é assertivo ao dizer que a violação de dados pessoais pode ser perigosa¹¹⁸. Nesse sentido o autor questiona se “os benefícios do presente

¹¹⁶ ALCANTARA, Larissa Kakizaki de. **Big Data e Internet das Coisas: desafios da privacidade e da proteção de dados no Direito Digital**. São Paulo: Independente, 2017. p. 28.

¹¹⁷ **APÓS** novo vazamento de dados, Google antecipa o fim do Google+. Disponível em: <https://info.wsouza.com.br/2018/12/apos-novo-vazamento-de-dados-fim-do-google-plus-e-antecipado.html>. Acesso em: 25 abr. 2020.

¹¹⁸ PASQUALE, Frank. **The Black Box Society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015. p. 29.

são melhores ou piores do que os custos do longo termo”¹¹⁹ e responde a própria indagação dizendo que “alguma mulher grávida pode estar satisfeita por receber cupons de desconto via *e-mail*, mas não a adolescente que ainda não contou a seus pais de sua gravidez”¹²⁰. A *internet* das coisas, assim, mecanismo que nasceu com o objetivo de garantir maiores facilidades àqueles que não possuíam tempo hábil para executar as tarefas mais simples do cotidiano, mostra-se como importante ferramenta de captura de dados pessoais¹²¹. O que importa, portanto, é se questionar, como fez Pasquale, sobre serem os benefícios do presente mais ou menos importantes que os custos ao longo prazo¹²² pela exposição dos usuários ao tratamento de dados feito pelas aplicações de IoT.

Em uma sociedade modernizada, onde as máquinas podem ser artificialmente tão inteligentes quanto os seres humanos, novos riscos surgem, com novos dilemas e novas proporções. Nesse contexto, a *internet* das coisas é capaz de transformar os tempos da alta modernidade em uma sociedade de risco. E esses riscos podem ser tanto abstratos quanto concretos. E, sendo concretos, podem se transformar em danos. Quem é o ator responsável para sopesar essa nova realidade? É o que trata o próximo ponto.

2.2 SOCIEDADE DE RISCO VIRTUALMENTE CONECTADA: TEMAS E PROBLEMAS DA INTERNET DAS COISAS EM APLICAÇÕES DE SAÚDE

Ulrich Beck, quando descreveu sua teoria da sociedade de risco, almejando mapear os rumos a outra modernidade, evoluiu sua análise social partindo dos contornos civilizatórios da sociedade de risco, passando pela individualização da desigualdade social através da destraditionalização das formas de vida da sociedade industrial, chegando à modernização reflexiva, ou seja, a generalização da ciência e da política. Para o sociólogo alemão, desde os primórdios da humanidade, viveu-se em uma *locus* habitada pelo risco, isto é, um contexto social

¹¹⁹ Tradução livre de: “Big data enables big danger. Are the present benefits worth the long-term costs?”. PASQUALE, Frank. **The Black Box Society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 29.

¹²⁰ Tradução livre de: “Some pregnant moms-to-be may be thrilled to get coupons tailored precisely to them. But not the teen who hadn’t yet told her father that she was pregnant”. *Idem*.

¹²¹ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 92.

¹²² PASQUALE, Frank. **The Black Box Society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 29.

que naturalizou “intervenções drásticas e ameaçadoras nas condições de vida das pessoas”¹²³. A sociedade de risco de Beck, em verdade, nada mais é do que uma realidade mundana em que se produz riscos e ameaças artificiais sobre as bases naturais da vida através de um processo de modernização social. E mais, para o autor, o processo de modernização da sociedade, inclusive no âmbito tecnológico, “torna-se reflexivo, convertendo-se a si mesmo em tema e problema”¹²⁴.

Nesse contexto de sociedade de risco, em que o processo de modernização produz perigos e ameaças artificiais sobre as bases naturais da vida, aliada ao desenvolvimento do conceito de *internet* das coisas, somando-se à busca pela saúde dos usuários de aplicações conectadas a IoT, como a evolução tecnológica pode considerar-se um tema e um problema ao mesmo tempo?

O desenvolvimento tecnológico é algo que se esquadrinha conquistar na época moderna. Toda a sociedade contemporânea está baseada no desenvolvimento tecnológico. Exemplo clássico disso é a Tesla Inc., empresa automotiva e de armazenamento de energia estadunidense que desenvolve, em seu portfólio, automóveis elétricos de alto desempenho. Em 2020, segundo notícia veiculada pela revista Forbes, a empresa presidida por Elon Musk, que fora fundada em 2003, atingiu um *equity* – somatório dos valores extrínseco e intrínseco de mercado – de aproximadamente US\$ 209,47 bilhões, superando a tradicional montadora japonesa Toyota cujo ano de fundação data de 1937¹²⁵. Mas o que faz a Tesla Inc. crescer tanto e tão depressa? A companhia foi a primeira montadora de carros a mostrar ser possível a confecção de um veículo automotor totalmente elétrico, não poluente e silencioso. Mais do que isso, a Tesla Inc., em sua corrida tecnológica, fez antes que outras montadoras os carros inteligentes, que se adaptam a seus condutores, dinamizam a experiência de dirigir, pensam e induzem tomadas de decisão tornando ainda mais segura e confortável a estadia dentro de um automóvel. Como consequência ao despontamento da Tesla Inc., outras corporações entraram nessa corrida automobilística. Dentre as principais encontra-se a Apple Inc., icônica companhia norte-americana criada por Steve Jobs, que

¹²³ BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011. p. 61.

¹²⁴ *Ibidem*. p. 24.

¹²⁵ FORBES. **Tesla supera Toyota como montadora com maior valor de mercado**. Disponível em <https://forbes.com.br/negocios/2020/07/tesla-supera-toyota-como-montadora-com-maior-valor-de-mercado/>. Acesso em 13 jan. 2021.

anunciou, em 2020, lançar seu primeiro protótipo ainda no ano de 2021, em parceria com a montadora sul coreana Hyundai¹²⁶.

Nessa mesma linha, pelo oitavo ano consecutivo, segundo levantamento realizado pela revista Exame, em 2020 a Apple Inc. figurou como sendo a marca mais valiosa do mundo¹²⁷. No rol das 10 empresas com mais valor de mercado do planeta, as cinco primeiras voltam-se ao ramo da tecnologia, estando listadas na NASDAQ, o balcão que negocia as ações das companhias de capital aberto que trabalham com tecnologia nos Estados Unidos. Atrás da Apple Inc. encontra-se a Amazon (sociedade empresária capitaneada por Jeff Besoz que, por meio do *Kindle*, comercializa *e-books*), a Microsoft de Bill Gates (desenvolvedora do sistema operacional mais utilizado no mundo, o *Windows*), o Google (principal plataforma de buscas virtuais do planeta), e, finalmente, a Samsung (mais forte concorrente da Apple Inc.)¹²⁸.

A justificativa para que essas empresas figurem a listagem das marcas mais valiosas do mundo está justamente na ascensão das empresas de tecnologia nos últimos anos.

De acordo com a Interbrand, isso é um efeito da pandemia e de momentos de crise, quando o “contrato” tácito entre organizações e pessoas é reformulado. Nesses momentos, o consumidor tende a exigir mais das marcas e começa a ver seu consumo como um voto de confiança. Com a ascensão das empresas de tecnologia nos últimos anos, diversas marcas perderam lugar no ranking, que é produzido desde 1988. Dessas 100, apenas 41 empresas já estavam nele no ano 2000.¹²⁹

Portanto, o desenvolvimento tecnológico é algo presente nos dias modernos. E qual é o porquê disso responde-se justamente porque a tecnologia, quando surge, possui como propósito facilitar a vida de quem a consome. Assim o é com a própria *internet* das coisas. Mas como a tecnologia se torna tema e problema, ao mesmo tempo, em uma sociedade de risco? É que, no momento em que a tecnologia – e, nesse caso, a *internet* das coisas e as aplicações de saúde – oferta a prestação de um serviço que hipoteticamente mostra-se como gratuito, há um preço a ser pago, o

¹²⁶ O GLOBO. **Apple e Hyundai vão se unir para construir carro elétrico autônomo**. Disponível em: <https://oglobo.globo.com/economia/apple-hyundai-va-se-unir-para-construir-carro-eletrico-autonomo-24831844>. Acesso em 13 jan. 2021.

¹²⁷ EXAME. **Apple se mantém como marca mais valiosa do mundo**. Disponível em: <https://exame.com/tecnologia/apple-se-mantem-como-marca-mais-valiosa-do-mundo-veja-ranking/>. Acesso em 13 jan. 2021.

¹²⁸ *Idem*.

¹²⁹ *Idem*.

que aponta o risco proveniente de um uso oculto desses dados que permeia essa sociedade da tecnologia. Beck afirma que, costumeiramente, o desenvolvimento e o emprego de novas tecnologias sobrepõem-se às questões de descoberta, integração, prevenção e acobertamento de riscos¹³⁰, quando, em verdade, o correto seria o oposto. E essa promessa de busca por facilidades, que é o mantra das aplicações conectadas a *internet* das coisas, para Beck, serve como argumento para sanar o que ele chama de ditadura da escassez.

Essa ditadura da escassez nada mais é do que a carência do material¹³¹, ou seja, a necessidade que sociedades têm de satisfazer-se com promessas de libertação de pobreza e sujeições imerecidas, de uma forma rápida, prática e pretensamente indolor. No contexto dos avanços tecnológicos que permeiam a chegada da *internet* das coisas, a ditadura da escassez está na adoção pela sociedade de mecanismos que antes se mostravam como desnecessários, porque as soluções eram analógicas, razão pela qual a libertação é a necessidade das sociedades em saciarem-se por meio de promessas de um horizonte digital mais automatizado e com menos ingerência humana. Beck diz que “essas promessas de libertação da pobreza e da sujeição imerecidas estão na base da ação, do pensamento e da investigação com as categorias da desigualdade social”¹³², haja vista que, em tais circunstâncias, na sociedade da escassez, “o processo de modernização encontra-se e consoma-se sob a pretensão de abrir com as chaves do desenvolvimento científico-tecnológico os portões que levam às recônditas fontes da riqueza social”¹³³.

Em que pese risco sempre existir, na história da humanidade, as aplicações conectadas à *internet* das coisas, e, nesse ponto, aquelas voltadas à saúde, possuem a aptidão de potencializar matematicamente seu alcance. Fortes denuncia que a proporção da atual sociedade de risco difere-se daquela que antes existia, porque, para ele, valendo-se de um exemplo de Beck, o desmatamento de uma floresta no passado causava apenas exploração inconsequente da madeira, quando, hoje, está pronto para desmatar florestas¹³⁴ e países, em razão da globalização.

¹³⁰ BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011. p. 24.

¹³¹ *Idem.*

¹³² *Idem.*

¹³³ *Idem.*

¹³⁴ FORTES, Vinícius Borges; REZER, Morgana Mezalira. Internet das coisas na sociedade de risco: uma análise a partir do direito à privacidade. In: CONGRESSO NACIONAL DO CONPEDI, XXVII,

Para Giddens, Beck e Lash, a ideia de risco está diretamente relacionada à ideia de evolução da tecnologia, haja vista que concedeu a todas as relações sociais uma mais larga rapidez e mais profunda complexidade, cuja gênese é o processo de industrialização e mundialização¹³⁵. E, precisamente, quando se trata do risco e sua dimensão de rede, Fortes admite um caráter de indeterminação¹³⁶, isto é, não se podendo determinar-se qual é o tamanho do risco que uma teia de computadores interconectados pode causar nas sociedades contemporâneas, dando conta da diferença entre os riscos do passado e os novos contornos da sociedade de risco no descortinar da rede mundial de computadores.

O tema, portanto, é a forma como as novas tecnologias de informação e comunicação, especialmente aquelas que se ligam à *internet* das coisas, habitam o cotidiano de seus usuários de modo a conferir-lhes facilidades que antes eram impensadas. Por outro lado, o problema é o risco que essa oferta de serviços pode expor quando o preço cobrado – porque nada é gratuito – traduz-se na cessão de valioso bem particular às aplicações virtuais, os dados pessoais.

Fato é que existe dois tipos de riscos, os concretos e os abstratos. Na doutrina de Colombo e Freitas, “enquanto os riscos concretos são diagnosticáveis pelo conhecimento científico vigente, os abstratos encontram-se em contextos de incerteza científica”¹³⁷. O risco abstrato nada mais é do que aquele medo imponderável, invisível à ciência jurídica e ao Direito. Conforme a teoria do risco abstrato, ser colocado em risco, ainda que por algo improvável, merece proteção e resposta do Poder Judiciário. O risco concreto, por sua vez, diz com ser posto em risco por algo que facilmente se possa prever acontecer. É um risco que, concretamente, é visto e sentido. Dentro da *internet* das coisas, pode-se visualizar ambos os riscos, abstrato e concreto. Magrani afirma que “transformar um objeto

2018, Porto Alegre. **Anais**. Porto Alegre. Disponível em <http://conpedi.danilolr.info/publicacoes/34q12098/9I053031/kFt980Gr7fWk908s.pdf>. Acesso em 13 jan. 2021. p. 106.

¹³⁵ GIDDENS, Anthony; BECK, Ulrich; LASH, Scott. **Modernização Reflexiva**. São Paulo: UNESP, 1997. p. 21.

¹³⁶ FORTES, Vinícius Borges; REZER, Morgana Mezalira. Internet das coisas na sociedade de risco: uma análise a partir do direito à privacidade. In: CONGRESSO NACIONAL DO CONPEDI, XXVII, 2018, Porto Alegre. **Anais**. Porto Alegre. Disponível em <http://conpedi.danilolr.info/publicacoes/34q12098/9I053031/kFt980Gr7fWk908s.pdf>. Acesso em 13 jan. 2021. p. 107.

¹³⁷ COLOMBO, Silvana; FREITAS, Vladimir Passos de. Da teoria do risco concreto à teoria do risco abstrato na sociedade pós-industrial: um estudo da sua aplicação no âmbito do direito ambiental. **Quaestio Iuris**, Rio de Janeiro, v. 8, n. 3, p. 1895-1912, out. 2015. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/18820>. Acesso em: 13 jan. 2021.

análogo em inteligente, além de encarecer o produto e deixa-lo sujeito a falhas que não teria *a priori*, pode gerar riscos também e em relação a segurança e a privacidade”¹³⁸. Nesse caso, está-se falando sobre o *big data*, ou seja, um volume massivo de dados sendo “processado, na escala de bilhões de dados diariamente, permitindo que seja possível conhecer cada vez mais os indivíduos em seus hábitos, preferências, desejos e tentando, assim, direcionar suas escolhas”¹³⁹.

Quando se discute o risco abstrato é justamente sobre o *big data* que se está a falar. Isso porque o usuário de alguma aplicação conectada à *internet* das coisas, ao ser alertado sobre a utilização de seus dados para a confecção de um *big data*, em um significativo número de casos, não se preocupa com a real consequência do mapeamento desses dados. Nesse sentido, atento a preocupação com os dados pessoais depositados na IoT, Magrani referencia valioso estudo¹⁴⁰ realizado pela universidade de Harvard, nos Estados Unidos, ainda no ano de 2015. Nesse experimento, os investigadores delataram, através de publicação na *Harvard Business Review*, que o principal entrave brasileiro frente à *internet* das coisas envolve o que se pode chamar de capacidade nacional de absorção – CNA¹⁴¹. Dentre os indicadores para se medir a capacidade nacional de absorção de cada país há a ética na utilização de dados pessoais dos usuários. E, segundo orienta Magrani, “a CNA do Brasil é bastante insatisfatória”¹⁴². Isso ocorre porque as empresas “não conseguiram garantir suficientemente a segurança e a privacidade dos dados com a mesma velocidade e empenho com que vêm desenvolvendo os dispositivos de IoT”¹⁴³.

Em recente investigação realizada pelo Instituto Ponemon em 17 países, a pedido da IBM *Security*, apontou-se que a violação de dados pessoais, no Brasil, causou prejuízo de R\$ 5,88 milhões às empresas brasileiras em 2020, o que representa um aumento de 10,5% em relação a 2019¹⁴⁴. Na média global, por sua

¹³⁸ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p. 35.

¹³⁹ *Idem*.

¹⁴⁰ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 77.

¹⁴¹ PURDY, Mark; DAVARZANI, Ladan; OVANESSOFF, Armen. **Como a Internet das Coisas Pode Levar à Próxima Onda de Crescimento no Brasil**. 2015. Disponível em: <https://hbrbr.uol.com.br/como-a-internet-das-coisas-pode-levar-a-proxima-onda-de-crescimento-no-brasil/>. Acesso em: 15 jun. 2019.

¹⁴² MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 78.

¹⁴³ *Ibidem*. p. 92.

¹⁴⁴ IBM. **How much would a data breach cost your business?**. Disponível em: <https://www.ibm.com/security/data-breach>. Acesso em: 14 jan. 2021.

vez, o valor apurado do prejuízo às empresas em razão da violação de dados pessoais é de US\$ 3,9 milhões. O Brasil é o país, dentre todos os 17 pesquisados “que mais tempo leva para identificar e conter um vazamento de dados: são 380 dias, ou 100 dias a mais do que a média dos demais países (280)”¹⁴⁵. Esses dados representam o quanto o país está atrasado, seja através de seus cidadãos, seja através de suas empresas, quando o assunto é proteção de dados pessoais.

Todavia, o conceito de *big data* não pode ser desconsiderado, posto que é fundamental para a compreensão da sociedade de risco moderna. Em pouco tempo, conforme alerta Magrani, a dimensão de gigabytes (uma medida de armazenamento de dados que equivale a um trilhão de *bytes*) será substituída por *zettabyte* (uma medida de armazenamento de dados que equivale a um sextilhão de *bytes*) ou até mesmo por *yottabyte* (uma medida de armazenamento de dados que equivale a 10^{24} *bytes*), haja vista a quantidade de informação armazenada¹⁴⁶. Para se ter uma noção, cada *byte* representa um único caractere de texto em um computador, o que materializa o tamanho da quantidade de informações com que o *big data* é capaz de nutrir-se.

Se não bastasse isso, a *Federal Trade Commission*, organização norte-americana responsável pela fiscalização e regulamentação do comércio estadunidense, demonstrou “preocupações com a segurança do ecossistema de IoT”¹⁴⁷. A organização estima que cerca de 10 mil habitantes, nos Estados Unidos, são capazes de gerar aproximadamente 150 milhões de *data points* diariamente¹⁴⁸. Um *data point* nada mais é do que todo e qualquer fato que tramita na *internet*, um *datum*, a forma singular dos dados¹⁴⁹. Isso quer dizer que, por dia, uma pequena cidade de 10 mil habitantes, no interior dos Estados Unidos, é capaz de produzir ou 150 milhões de quaisquer coisas na rede mundial de computadores, ou 150 milhões de cliques em quaisquer sítios virtuais, ou 150 milhões de curtidas e compartilhamentos em quaisquer redes sociais. E o mais preocupante é que esse

¹⁴⁵ FEBRABAN. **Empresas brasileiras perdem quase R\$ 6 mi com vazamento de dados**: Brasil é o país que mais tempo leva para identificar e conter incidentes de segurança, diz estudo global da IBM Security. Disponível em: <https://noomis.febraban.org.br/noomisblog/empresas-brasileiras-perdem-quase-r-6-mi-com-vazamento-de-dados>. Acesso em: 14 jan. 2021.

¹⁴⁶ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 22.

¹⁴⁷ MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p. 35.

¹⁴⁸ *Ibidem*. p. 36.

¹⁴⁹ DATA POINT. Disponível em: <https://whatis.techtarget.com/definition/data-point>. Acesso em 13 jan. 2021.

número se renova a cada dia. O problema, segundo Magrani, é que o tratamento desses dados ainda não é uma preocupação tão grande para as empresas de IoT quanto desenvolver novas aplicações possa ser¹⁵⁰. Assim, todo o usuário de aplicativos conectados à *internet* das coisas está sujeito à produção de dados, mas poucos são os usuários que sabem ou possuem controle sobre os seus dados pessoais produzidos.

A equação é simples: quando se acessa a rede mundial de computadores, necessariamente se produz rastros. Tudo o que se faz na rede deixa rastros. Esses rastros são conhecidos como dados e englobam o que se chama de *big data*. Magrani diz que “todos os dias, as coisas se conectam à *internet* com capacidade para compartilhar, processar, armazenar e analisar um volume enorme de dados entre si”¹⁵¹ e que essa prática é o que “une o conceito de IoT ao de *big data*”¹⁵². O risco abstrato, portanto, escancara-se quando o CNA brasileiro é insatisfatório, porque imprevisível e invisível, mas audaciosamente presente na *internet* das coisas. Já o risco concreto, por sua vez, não está mais no *big data*, mas, sim, na forma como esse volumoso emaranhado de dados é utilizado. Se o risco concreto diz com ser colocado em risco por algo que facilmente se possa prever acontecer, Magrani enumera quatro riscos principais relacionados à *internet* das coisas: identificação, rastreamento, *profiling* e *lifecycle*.

O primeiro risco, a identificação, está associado aos dados de identidade de alguém. Conforme diz Magrani, “as tecnologias inseridas no contexto da IoT seriam mais sujeitas a esse risco devido às possibilidades de identificação facial e por meio das digitais dos indivíduos”¹⁵³. E sobre a identificação facial, um interessante exemplo da vulnerabilidade dos dispositivos interligados com a *internet* das coisas é denunciado por Martins. A autora diz que a utilização de aplicações conectadas à *internet* das coisas ligadas à saúde pode configurar o que se entende por monitorização contínua¹⁵⁴, isto é, um sistema onde quem está se valendo da tecnologia de IoT para controle de sua saúde é monitorado ininterruptamente, a fim

¹⁵⁰ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 92.

¹⁵¹ *Ibidem*. p. 22.

¹⁵² *Idem*.

¹⁵³ *Ibidem*. p. 96.

¹⁵⁴ MARTINS, Joana Castel-Branco Saldanha. **A Internet das Coisas em Serviços de Saúde**. 137 f. Dissertação (Mestrado) – Faculdade de Economia e Gestão, Universidade Católica Portuguesa, Porto, 2019. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/28405/1/TFM_JoanaSaldanha.pdf. Acesso em: 17 dez. 2020. p. 56-57.

de que, sendo detectada alguma emergência o sistema de saúde seja prontamente acionado. Para Martins, em “algumas situações, os doentes precisam de monitorização de longo-prazo, principalmente quando se tratam de doenças crónicas [sic]”¹⁵⁵. A consequência disso é que, em “um mundo onde tudo está conectado, onde a informação é comunicada, onde os dados são recolhidos [...] faz com que uma porta se abra para um *Big Brother*”¹⁵⁶. Em aplicações ordinárias de IoT, que não envolvam a perfectibilização da saúde do usuário, o mesmo ocorre. É exemplo a plataforma Insecam. Navegando pelo sítio¹⁵⁷, o usuário tem acesso momentâneo a incontáveis câmeras em tempo real ao redor do mundo. Dito acesso é conferido ao *site* uma vez que as câmeras se valem de senhas-padrão, descritografadas pela plataforma e disponibilizadas na rede mundial de computadores. Assim, aquela câmera de vigilância acoplada em uma hipotética residência, com o objetivo de garantir maior segurança aos moradores da casa, se conectada à rede mundial de computadores para armazenar as imagens na nuvem, provavelmente estará vulnerável ao Insecam. Segundo Magrani, “a ideia do *site* [...] é criar um alerta para a privacidade *online* e a importância de mudar as senhas a partir da exposição não autorizada dessas imagens”¹⁵⁸. Todavia, há imagens disponibilizadas no sítio de pessoas assistindo televisão na sala de suas casas, por exemplo.

O segundo risco apontado é o rastreamento, que possibilita sejam identificadas as localizações dos indivíduos que se ocupam do ciberespaço. Para Magrani, “o principal receio de diversos estudiosos da IoT, quando se está a tratar dessa questão, deve-se ao fato de que os usuários não têm o controle sobre esse tipo de dado”¹⁵⁹. O lugar onde estão os usuários é captado muitas vezes sem o seu consentimento, e esse dado muito provavelmente é tratado a sua revelia. Martins pondera que uma das principais preocupações com a evolução das tecnologias IoT na área da saúde é a segurança da informação pessoal de pacientes, porque, em tempo real as aplicações de IoT em saúde “capturam e partilham *data* na *cloud* para

¹⁵⁵ MARTINS, Joana Castel-Branco Saldanha. **A Internet das Coisas em Serviços de Saúde**. 137 f. Dissertação (Mestrado) – Faculdade de Economia e Gestão, Universidade Católica Portuguesa, Porto, 2019. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/28405/1/TFM_JoanaSaldanha.pdf. Acesso em: 17 dez. 2020. p. 56-57.

¹⁵⁶ *Ibidem*. p. 56.

¹⁵⁷ Pode-se consultar a plataforma através do *link* <http://www.insecam.org>.

¹⁵⁸ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 96.

¹⁵⁹ *Ibidem*. p. 98.

fins de *data analytics*¹⁶⁰, e essa informação, segundo a autora, recolhida dos “*wearables* é preciosa para ciber-criminosos que podem explorar os dados roubados para seu próprio proveito”¹⁶¹. E o exemplo é justamente esse: a captura de dados de rastreamento para o cometimento do crime de extorsão. Em que pese não haver notícia ainda, quem pode duvidar de eventual tratamento de dados feito pela Tesla Inc. nos veículos que se valem da IoT para navegarem via sistema de geolocalização?

Por sua vez, o terceiro risco refere-se ao *profiling*, isto é, a “criação de dossiês de informações sobre determinado indivíduo com o intuito de efetuar correlações com outras informações e perfis”¹⁶². Esse risco à privacidade evidencia-se a partir do compartilhamento de dados com terceiros eventualmente não autorizados, aonde o tratamento desses dados é capaz de formar uma teia de informações a ponto de monitorar todo o perfil do usuário. Essa possibilidade, o *profiling*, fora pontualmente analisada pelo mercado de consumo, que costuma o explorar através do que se conhece por *target marketing*. O *target marketing* nada mais é do que a publicidade direcionada, ou seja, “a possibilidade de personalização e customização automática de conteúdo nas plataformas digitais, inclusive capitalizando essa filtragem com publicidade direcionada por meio de rastreamento de *cookie*”¹⁶³.

No caso dos dados pessoais sensíveis de saúde, o risco referente ao *profiling* toma novos contornos. É que o reconhecimento da qualidade dos dados de saúde como sendo dados pessoais sensíveis, especialmente pela Lei Geral de Proteção de Dados Pessoais brasileira, se deu justamente porque as informações médicas e biométricas de indivíduos que utilizam dispositivos conectados às aplicações da *internet* das coisas pode levar a discriminação desses titulares de dados pessoais a partir da análise e do mapeamento desses dados, impactando severamente a vida desses usuários. É que a criação desses dossiês de informações sobre o indivíduo titular dos dados pessoais sensíveis de saúde, com a correspondente correlação com outras informações e perfis desse mesmo usuário, desenhando seu *profiling*,

¹⁶⁰ MARTINS, Joana Castel-Branco Saldanha. **A Internet das Coisas em Serviços de Saúde**. 137 f. Dissertação (Mestrado) – Faculdade de Economia e Gestão, Universidade Católica Portuguesa, Porto, 2019. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/28405/1/TFM_JoanaSaldanha.pdf. Acesso em: 17 dez. 2020. p. 57.

¹⁶¹ *Idem*.

¹⁶² MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 98.

¹⁶³ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p. 35.

segundo Martins, pode servir como máscara a um *hacker* criar um ID falso desse paciente para o cometimento de extorsão, ou para a compra de medicamentos indevidos ou mesmo equipamentos médicos para o cometimento de outros crimes sempre em nome do próprio usuário titular dos dados de saúde¹⁶⁴. E todas essas práticas se originam a partir da coleta de dados pessoais sensíveis de saúde a partir de aplicações conectadas à *internet* das coisas.

Por último, o quarto risco à privacidade dos usuários de aplicações de *internet* das coisas chama-se *lifecycle* da tecnologia, sobretudo quando liberada alguma informação do usuário. Isto é, os “objetos inseridos na tecnologia de IoT terão um *lifecycle* bem mais dinâmico, no qual os objetos serão descartados, modificados e emprestados de forma mais flexível”¹⁶⁵. O risco está no sentido de que os dados armazenados por um dispositivo permanecem no dispositivo utilizado. Ocorre que, ao se descartar ou emprestar o aparelho, por exemplo, descarta-se e empresta-se o aparelho com os dados pessoais do então usuário inseridos em seu *software*, razão pela qual eles poderiam ser facilmente tratados pelos novos possuidores daquele dispositivo.

É importante apontar que muitos dos dados capturados podem interferir inclusive no futuro de pessoas que não detém capacidade de escolha. É que a utilização de vestíveis, por exemplo, os *gadgets* e os *warables* que capturam dados médicos, quando feita por crianças e adolescentes, não diz com sua manifestação de vontade em postular o uso do vestível. Em algumas vezes os próprios pais dos usuários manejam a utilização desses dispositivos em seus filhos, ou utilizam em si capturando dados que dirão com o futuro dessas crianças e adolescentes. E, conseqüentemente, a formação desses perfis e a manutenção desses dados, especialmente quando se trata de dados provenientes daqueles que não possuem capacidade de escolha, ainda que com o argumento da promoção da saúde coletiva, pode ferir gravemente os direitos fundamentais individuais de seus titulares. Se não bastasse isso, feridos os direitos individuais, abre-se um caminho para o desmoronamento completo da democracia. Agamben, nesse sentido, aponta que perigos como o desmoronamento completo da democracia podem ser concretizados

¹⁶⁴ MARTINS, Joana Castel-Branco Saldanha. **A Internet das Coisas em Serviços de Saúde**. 137 f. Dissertação (Mestrado) – Faculdade de Economia e Gestão, Universidade Católica Portuguesa, Porto, 2019. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/28405/1/TFM_JoanaSaldanha.pdf. Acesso em: 17 dez. 2020. p. 57.

¹⁶⁵ MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018. p. 99.

em razão de um constante estado de exceção¹⁶⁶. O *surveillance*, isto é, a vigilância constante cuja gênese se dá na desproteção de dados pessoais, e especialmente na fragilidade dos dados pessoais sensíveis de saúde, onde, sob o manto da segurança da saúde física se concorda com que todos os seus dados sejam monitorados, cria o que Bolzan chama de cidadão securitizado¹⁶⁷. Dessa forma, a obtenção e o tratamento de dados pessoais serve não apenas para o mercado, mas também para contornos políticos bastante gravosos.

Ao analisar os riscos abstrato e concreto, Beck salienta que, sob a ótica do impacto, essas facetas da teoria do risco consumam-se no reconhecimento dos perigos da modernização e através da aplicação dos cuidados que neles estão contidos, acarretando em uma mudança sistêmica¹⁶⁸. Todavia, ocorre “não abertamente, mas sob a forma de uma “revolução silenciosa”, como consequência da mudança de consciência de todos, como subversão *sem* sujeito”¹⁶⁹. Isso significa que essa mudança sistêmica faz com que se normalize, por parte dos usuários de aplicações conectadas à *internet* das coisas, a captura de seus dados. Essa alimentação do *big data* vem à tona de forma silenciosa, transgressora e sorrateira, com a formação de um enorme banco de dados e a confecção de identificação, rastreamento, *profiling* e *lifecycle* de maneira natural e habitual para quem opta por vender-se como parte desse enredo de interconexões. Nesse sentido, no desenfreio civilizatório do processo de modernização da sociedade de risco,

são simultaneamente *designadas* situações semirrevolucionárias. Elas surgem como “destino civilizacional”, outorgado pela modernização, e em consequência, por um lado sob o manto da *normalidade* e, por outro lado, com o *penhor de catástrofes*, perfeitamente capaz, por conta da ampliação dos perigos, de igualar e ultrapassar o raio constitutivo de uma revolução. A sociedade de risco não é, portanto, um [sic] sociedade revolucionária, mas mais do que isto: uma sociedade *catastrofal*. Nela, o *estado de exceção* ameaça converter-se em *normalidade*.¹⁷⁰

A sociedade de risco, na sociedade da informação, é naturalizada, relativizada. O problema é mitigado pelo tema. Em nome das incontáveis benesses

¹⁶⁶ AGAMBEN, Giórgio. **Estado de exceção**. São Paulo: Boitempo, 2004. p. 15.

¹⁶⁷ MORAIS, José Luis Bolzan de. O Estado de Direito como mecanismo político-jurídico do liberalismo. In: MORAIS, José Luis Bolzan de; LOBO, Edilene (Orgs.). **Temas de Estado de Direito e Tecnologia**. Porto Alegre: Editora Fi, 2001. p. 26.

¹⁶⁸ BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade**. 2. ed. São Paulo: Editora 34, 2011. p. 96.

¹⁶⁹ *Idem*.

¹⁷⁰ BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade**. 2. ed. São Paulo: Editora 34, 2011. p. 96.

da *internet* das coisas, das novas tecnologias de informação e comunicação, da rede mundial de computadores como um todo, releva-se a formação do *big data*, releva-se o risco abstrato e releva-se o risco concreto. Acontece que essa naturalização dos riscos, em nome de um desenvolvimento tecnológico, e especialmente do desenvolvimento tecnológico de aplicações com o intuito de aprimoramento da saúde de seus usuários, com *status* de ser o destino civilizacional dos novos tempos, pode fazer com que essa sociedade, que nasceu informacional e é do risco, se transforme rapidamente em uma sociedade da catástrofe, em que se ultrapassa o raio constitutivo da revolução tecnológica, tornando o usuário da rede como o principal alimentante, através da cessão de seus dados pessoais por meio da rede mundial de computadores. Fato é que, seja pelo mais volátil ciclo de vida das aplicações de IoT, seja pela localização dos usuários ou pela montagem de perfis desses usuários, a *internet* das coisas mostra-se como uma ferramenta hábil a transgressão dos dados pessoais (e, se tratando de aplicações de IoT voltadas à saúde, de dados pessoais sensíveis) de quem a desfruta, através suas coletas, tratando-os e cruzando-os com dados capturados por outros dispositivos, mostrando-se capaz de mapear toda a vida passada, presente e futura de uma pessoa.

Superando a sociedade de riscos, os riscos pode se transformar em danos. Em importante obra sobre a proteção de dados pessoais, Vaidhyathan entende que aqueles que se utilizam das plataformas do *Google*, são “usuários”, ao passo em que, ao compreenderem que estão utilizando a rede de forma gratuita, destinam seus dados pessoais como contraprestação às informações pelo *Google* disponibilizadas, uma verdadeira forma de pagamento¹⁷¹. Os dados, por sua vez, são objeto de venda pelo *Google* aos anunciantes, seus reais clientes:

Na era anterior ao Google, as empresas criavam produtos que vendiam aos clientes por meio de uma propaganda que levava informações a compradores potenciais. O Google reconfigurou totalmente esse modelo. Seu próprio produto, como afirmei, é na verdade a atenção e a lealdade de seus usuários. Ao mesmo tempo que fornece a seus usuários as informações que eles procuram, aparentemente sem cobrar por elas, o Google coleta os *gigabytes* das informações pessoais e o conteúdo criativo que milhões de usuários seus fornecem gratuitamente à rede todos os dias,

¹⁷¹ VAIDHYANATHAN, Siva. **A Googlelização de Tudo:** (e por que devemos nos preocupar, a ameaça do controle total da informação por meio da maior e mais bem-sucedida empresa do mundo virtual. São Paulo: Cultix, 2011. p. 40.

e vende essas informações a anunciantes de milhões de produtos e serviços.¹⁷²

É assim que os riscos transformam-se em danos. Quando se discute as aplicações vinculadas à *internet* das coisas que mapeiam os dados de saúde de seus usuários, o primeiro dano, que bem se pode conectar ao mais singelo equívoco que o tratamento desenfreado de um *big data* possa causar, é o vazamento de dados pessoais. Em 2020, no enfrentamento da pandemia causada pela disseminação descontrolada do Sars-CoV-2, o coronavírus causador da COVID-19, o Hospital Albert Einstein, uma das principais instituições de saúde do Brasil, armazenou incontáveis dados de pacientes contaminados pela doença. Esses dados iam desde a gravidade da moléstia para aquele determinado sujeito, se leve, moderada ou grave, até mesmo o histórico clínico de internações dessas pessoas. E isso acontecia porque o Hospital Albert Einstein utilizava dois sistemas que montavam esse *big data*, ambos oriundos do governo federal brasileiro: o E-SUS-VE, onde eram notificados os casos suspeitos e confirmados da COVID-19, além da complexidade que a doença tomara naquele organismo, e o Sivep-Gripe, *software* onde se registrava todas as internações por síndrome respiratória aguda grave¹⁷³. Se não bastasse isso, informações pessoais dos pacientes, como o apontamento de doenças pré-existentes, a exemplo da diabetes e da hipertensão, problemas cardíacos, cânceres e contaminações pelo vírus HIV, além de históricos clínicos preliminares, também foram violados¹⁷⁴.

O incidente no Hospital Albert Einstein, em São Paulo se deu em maio de 2020 e afetou nada menos do que 16 milhões de pessoas, enfermos da rede pública e privada, haja vista o cruzamento de dados de todos os pacientes, ao longo do país, que comunicaram testagens positivas e negativas da COVID-19 ao sistema de saúde. Durante quase um mês,

um vazamento de senhas de sistemas do Ministério da Saúde deixou exposto da *internet* dados pessoais e médicos de ao menos 16 milhões de brasileiros que tiveram diagnósticos suspeitos ou confirmados de COVID-

¹⁷² *Idem.*

¹⁷³ PRIVACY TECH. **Vazamento no Ministério da Saúde expõe dados de 16 milhões de pacientes de COVID.** Disponível em: <https://privacytech.com.br/destaque/vazamento-no-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid.,381009.jhtml>. Acesso em 14 jan. 2021.

¹⁷⁴ PRIVACY TECH. **Vazamento no Ministério da Saúde expõe dados de 16 milhões de pacientes de COVID.** Disponível em: <https://privacytech.com.br/destaque/vazamento-no-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid.,381009.jhtml>. Acesso em 14 jan. 2021.

19. Os dados expostos incluíam informações como CPF, endereço, telefone e doenças pré-existentes. Entre as pessoas afetadas pelo vazamento estão inclusas o presidente Jair Bolsonaro e seus familiares; Eduardo Pazuello, ministro da Saúde; João Dória, governador de São Paulo e diversos nomes da política, como Onyx Lorenzoni, Damares Alves e Rodrigo Maia.¹⁷⁵

Além disso, o vazamento de dados ocorrido no Hospital Albert Einstein se deu porque um funcionário da casa hospitalar divulgou a lista de *logins* e senhas de acesso de cada um desses usuários ao *big data* da instituição. Ciente disso, o problema agravou-se quando o jornal Estadão, também de São Paulo, divulgou um *link* do DataSUS, banco de dados do Sistema Único de Saúde, onde as chaves de acesso foram apresentadas¹⁷⁶, pulverizando ainda mais a falha na segurança da informação do hospital. Se pudesse ser crível que o problema não se repetiria, em dezembro de 2020, isto é, poucos meses depois, o Ministério da Saúde informou a ocorrência de nova falha de segurança de dados¹⁷⁷. Todavia, nesse segundo acontecimento foram expostos registros de cerca de 243 milhões de brasileiros – um cálculo que envolve, inclusive, dados de pessoas já falecidas.

Quanto às aplicações diretamente ligadas à *internet*, ainda no enfrentamento da pandemia causada pelo Sars-CoV-2, tornou-se comum, ao longo de 2020, a utilização por governos de dados de localização de aparelhos celulares a fim de que controlar possíveis aglomerações de pessoas. Enquanto a COVID-19 se espalhava pelo planeta, gestores públicos ao redor de todo o mundo buscavam medidas para conter a transmissibilidade do vírus. Uma das formas imaginadas era através da identificação de pessoas potencialmente contaminadas somadas ao mapeamento de seu lastro. Uma importante ferramenta para a concretização dessa estratégia (o monitoramento de pessoas) estava acoplada junto a uma grande parcela da população mundial, mais precisamente no bolso das pessoas: os aparelhos *smartphones*, uma das principais alternativas de conectividade da *internet* das

¹⁷⁵ *Idem*.

¹⁷⁶ ESTADÃO. **Vazamento de senha do Ministério da Saúde expõe dados de 16 milhões de pacientes de COVID**. Disponível em: <https://saude.estadao.com.br/noticias/geral,vazamento-de-senha-do-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid,70003528583>. Acesso em 14 jan. 2021.

¹⁷⁷ PRIVACY TECH. **Mais de 200 milhões de brasileiros têm dados pessoais expostos em nova falha de segurança do Ministério da Saúde**. Disponível em: <https://privacytech.com.br/destaque/mais-de-200-milhoes-de-brasileiros-tem-dados-pessoais-expostos-em-nova-falha-de-seguranca-do-ministerio-da-saude.,381645.jhtml>. Acesso em 14 jan. 2021.

coisas¹⁷⁸. Através da utilização da geolocalização por sistemas de GPS dos usuários de aparelhos celulares inteligentes, os governos puderam mapear a circulação de pessoas em potenciais focos de contaminação do vírus.

Exemplo clássico disso ocorreu na Coreia do Sul. Desde o momento em que o governo sul coreano se deu conta da gravidade do Sars-CoV-2, testou em massa sua população, buscando o isolamento monitorado através do sinal de GPS de *smartphones* desses pacientes da COVID-19. Só que o governo sul coreano não parou por aí. Quando o enfermo contaminava-se com o vírus, o primeiro passo era o mapeamento via GPS, mas, em um segundo estágio, o Estado passava a controlar, inclusive, o histórico de uso do cartão de crédito¹⁷⁹, permitindo ter-se conhecimento, inclusive, dos estabelecimentos comerciais visitados pelo contaminado.

Ao se valer do discurso de controle pandêmico, esquece-se, por outro lado, as facetas negativas dessa abordagem. A primeira delas, e talvez mais óbvia, é a violação à privacidade. Se o tema, lembrando Beck, é a busca pela saúde da coletividade, o problema é que não se consulta a coletividade sobre o preço – a cessão de dados pessoais – a ser pago. A *Electronic Frontier Foundation*, fundação privada estadunidense que fiscaliza a utilização de dados pessoais captados através de dispositivo eletrônicos ao redor do globo, defendendo uma série de temas relacionados à privacidade digital, realizou um emaranhado de denúncias sobre a *surveillance* no uso de dados de geolocalização. Uma das observações diagnosticadas é de que, se em um país muitas são as testagens positivas para infecção pelo Sars-CoV-2, não se consegue mapear a forma como se deu essa massiva contaminação¹⁸⁰.

Então qual seria o real motivo, que se transforma em um efetivo dano, para o mapeamento de geolocalização? A *Electronic Frontier Foundation* denuncia que empresas estão criando plataformas virtuais de trabalho remoto, em nome da contingência de infecções, fomentando os *home offices* sob a toga da produtividade, mas, em verdade, se trata da criação de uma listagem, com análise e pontuação da

¹⁷⁸ FORNASIER, Mateus de Oliveira. The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy. *Rev. Investig. Const.*, Curitiba, v. 6, n. 2, p.297-321, maio 2018. Disponível em: <https://revistas.ufpr.br/rinc/article/view/67592/39878>. Acesso em: 17 abr. 2021. p. 302.

¹⁷⁹ OLHAR DIGITAL. **Como governos estão usando dados de localização dos celulares no combate à Covid-19**. Disponível em: <https://olhardigital.com.br/2020/03/28/noticias/como-governos-estao-usando-dados-de-localizacao-dos-celulares-no-combate-a-covid-19/>. Acesso em 14 jan. 2021.

¹⁸⁰ EFF. **COVID-19 and surveillance tech: year in review 2020**. Disponível em: <https://www.eff.org/pt-br/deeplinks/2020/12/covid-19-and-surveillance-tech-year-review-2020>. Acesso em 14 jan. 2021.

real forma de trabalhar das pessoas, a fim de que se possa analisar esses perfis em busca de realizar ou não novas contratações¹⁸¹:

estados também estão fazendo parceria com empresas para criar *sites* onde os trabalhadores fornecem informações sobre sua saúde e exames para testes e tratamento da COVID-19. Assim como o *Department of Health and Human Services* dos Estados Unidos expandiu seu processamento de dados sobre pessoas que fizeram os testes COVID-19, o governo federal anunciou planos para compartilhar esses dados com as corporações americanas, incluindo *TeleTracking Technologies* e *Palantir*. As empresas também estão expandindo sua vigilância sobre os trabalhadores. Isso ocorre em locais de trabalho, em nome do rastreamento de infecções, e em escritórios domésticos socialmente distantes, em nome do rastreamento da produtividade.¹⁸²

Práticas como essas fizeram com que, na Coreia do Sul, segundo jornal o *The Washington Post*¹⁸³, algumas pessoas preferissem não buscar atendimentos à COVID-19 nem testes detectores de infecção do Sars-CoV-2, porque “onde algumas pessoas percebiam boas intenções outras viam um *Big Brother*”¹⁸⁴. No Brasil cidades e estados firmaram contratos com companhias de telefonia móvel ou desenvolvedoras de aplicativos para *smartphones* com o mesmo objetivo, o monitoramento por geolocalização. Segundo a *In Loco*, principal desenvolvedora de aplicativos para celular no país, contratada pelos governos de Alagoas, Amapá, Amazonas, Ceará, Maranhão, Goiás, Mato Grosso do Sul, Mato Grosso, Minas Gerais, Pará, Paraíba, Piauí, Santa Catarina e Rio Grande do Sul, além das prefeituras de Recife, Teresina e Aracajú, a adesão dos usuários de *smartphone*

¹⁸¹ *Idem*.

¹⁸² Tradução livre de: “States are conducting manual contact tracing, often contracting with business to build new data management systems. States also are partnering with businesses to create websites where we provide our health and other information to obtain screening for COVID-19 testing and treatment. Just as the U.S. Department of Health and Human Services expanded its processing of data about people who took COVID-19 tests, the federal government announced plans to share COVID-related data with its own corporate contractors, including TeleTracking Technologies and Palantir. Businesses are also expanding their surveillance of workers. This occurs at job sites, in the name of tracking infection, and in socially distant home offices, in the name of tracking productivity”.

Idem.

¹⁸³ THE WASHINGTON POST. **A ‘travel log’ of the times in South Korea: Mapping the movements of coronavirus carriers.** Disponível em: https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html. Acesso em 14 jan. 2021.

¹⁸⁴ Tradução livre de: “But where some people perceive good intentions, others see Big Brother”. THE WASHINGTON POST. **A ‘travel log’ of the times in South Korea: Mapping the movements of coronavirus carriers.** Disponível em: https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html. Acesso em 14 jan. 2021.

deveria ser voluntária e consciente¹⁸⁵, mesmo que não se tenha relatos, na prática, de consulta a esses titulares de dados pessoais sobre seu interesse ou não na cessão de seus dados de geolocalização.

Merece especial atenção caso brasileiro. É que, desde 18 de setembro de 2020, a Lei Geral de Proteção de Dados Pessoais, levada à efeito sob o número 13.709, está vigente no país. Os fundamentos da LGPD, que estão esculpidos no artigo segundo dessa norma jurídica, norteiam a aplicação da legislação em busca do respeito à privacidade, da autodeterminação informativa, da liberdade de expressão, informação, comunicação e opinião, da inviolabilidade da intimidade, da honra e da imagem, do desenvolvimento econômico, tecnológico e da inovação, da livre iniciativa, da livre concorrência e da defesa do consumidor e dos direitos humanos, do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania pelas pessoas.

Como se pode perceber, a Lei Geral de Proteção de Dados Pessoais brasileira está estritamente ligada à preservação da privacidade. Além disso, a autodeterminação informativa, ou seja, a faculdade que o titular de um dado pessoal tem de controlar toda e qualquer informação que diga a seu respeito, passou a ser o norte básico do tratamento de dados pessoais no Brasil a partir da vigência da LGPD. Ocorre que, conforme se demonstrará oportunamente, dentre as bases legais para o tratamento de dados pessoais previstas no artigo sétimo da lei número 13.709 pode-se questionar se a LGPD é conivente ou não com o tratamento desenfreado de dados pessoais que envolvam a saúde do titular e da coletividade. Assim, no caso brasileiro, ainda que haja uma legislação que tutele a proteção de dados – e, nesse ponto, conseqüentemente, os dados de geolocalização de *smartphones*, por exemplo, para o contingenciamento pandêmico – a interpretação legislativa pode-se mostrar em certa medida talvez ineficaz para a tutela da privacidade.

Outras são as aplicações vinculadas à *internet* das coisas que transformam riscos abstratos e riscos concretos em efetivos danos. Recentemente, clínicas de Portugal recusaram cuidados a doentes que desautorizaram o tratamento de seus dados pessoais. No caso português, quatro institutos de saúde, o Centro Hospitalar

¹⁸⁵ BBC. **Coronavírus:** uso de dados de geolocalização contra a pandemia põe em risco sua privacidade?. Disponível em: <https://www.bbc.com/portuguese/brasil-52357879>. Acesso em 14 jan. 2021.

São Francisco, o Somardental Serviços Policlínicos, a Clidiral – Clínica de Diagnóstico e Radiologia, e o Valentim Ribeiro – Hospital de Esposende, “recusaram-se a prestar cuidados de saúde a doentes que não quiseram assinar declarações de consentimento relativas ao tratamento de dados pessoais”¹⁸⁶. O Centro Hospitalar São Francisco e o Somardental Serviços Policlínicos negaram tratamento médico aos pacientes, porque entendiam necessitar obter a concordância do adoentado para que realizassem o tratamento de dados inerentes ao serviço de saúde que prestariam. Já, de forma mais radical, a Clidiral e o Valentim Ribeiro negaram tratamento porque exigiam a firma de um termo de consentimento para tratar todo e qualquer dado pessoal do paciente – mesmo aqueles que não envolvessem a saúde do titular dos dados.

Provocada a se manifestar no caso concreto, a autoridade nacional de proteção de dados pessoais portuguesa emitiu, em maio de 2020, um parecer, onde considerou o comportamento de ambas as clínicas e de ambos os hospitais como sendo abusivo, já que violam o Regulamento Geral de Proteção de Dados europeu. O fundamento legal é que, conforme o RGPD, nem sempre é necessário obter o consentimento para o tratamento de dados pessoais, como no caso dos tratamentos de dados de saúde¹⁸⁷. À luz do artigo nono do regulamento europeu, “não é necessário obter consentimento para o tratamento de dados pessoais no âmbito da prestação de cuidados de saúde (onde se incluem o diagnóstico médico e a terapêutica)”¹⁸⁸. Por essa razão, não se justificaria a negativa dos hospitais e clínicas, haja vista que a possibilidade de prestação do serviço médico independentemente da firma de um termo de consentimento para o tratamento de dados de saúde.

No Brasil, em 2019, formou-se uma comissão na Câmara dos Deputados a fim de discutir a medida provisória número 869, de 27 de dezembro de 2018, que possuía, dentre outros objetivos, alterar a LGPD para dispor sobre a proteção de dados pessoais e criar a Autoridade Nacional de Proteção de Dados, além de debater o compartilhamento e a proteção de dados na saúde e na pesquisa

¹⁸⁶ EXPRESSO. **Clínicas recusaram cuidados a doentes que disseram não ao tratamento de dados pessoais**. Disponível em: <https://expresso.pt/economia/2019-06-08-Clinicas-recusaram-cuidados-a-doentes-que-disseram-nao-ao-tratamento-de-dados-pessoais>. Acesso em 15 jun. 2019.

¹⁸⁷ *Idem*.

¹⁸⁸ EXPRESSO. **Clínicas recusaram cuidados a doentes que disseram não ao tratamento de dados pessoais**. Disponível em: <https://expresso.pt/economia/2019-06-08-Clinicas-recusaram-cuidados-a-doentes-que-disseram-nao-ao-tratamento-de-dados-pessoais>. Acesso em 15 jun. 2019.

científica. Em abril de 2019, durante a sétima reunião de debates, discutiu-se um relatório que fora apresentado pelo então deputado federal Orlando Silva, cujo mérito dizia com a flexibilização para o compartilhamento de dados de saúde. Esse relaxamento buscava a autorização da divisão de dados sem o consentimento de seu titular. A medida provisória, por outro lado, manteve-se originalmente inerte, alterando a redação da Lei Geral de Proteção de Dados Pessoais, que ainda não estava vigente no país, para que constasse, à época, no inciso segundo do parágrafo quarto do artigo 11 da norma, que é vedada a comunicação ou o uso compartilhado entre controladores de “dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de necessidade de comunicação para a adequada prestação de serviços de saúde suplementar”¹⁸⁹.

Os serviços de saúde suplementar nada mais são do que as atividades que possam trafegar por planos de saúde e por seguros privados de assistência médica à saúde. A operação dos serviços de saúde suplementar é fiscalizada, no Brasil, pela Agência Nacional de Saúde Suplementar. A ANS regulamenta que as operadoras são seguradoras especializadas em saúde, medicinas de grupo, instituições filantrópicas e autogestões e cooperativas. Um dos principais objetivos dessa associação é justamente a organização de um fundo mútuo, o que quer dizer que, inclusive, a avaliação do risco e a definição do preço são organizados pela ANS¹⁹⁰. Em razão disso, durante a quarta audiência pública, a presidente do Instituto de Pesquisa em Direito e Tecnologia do Recife

alertou para a possibilidade de aumentos abusivos, algoritmos obscuros e negativas de tratamento, como resultado de compartilhamento sob alegada “adequada prestação”, termos que, para ela, são considerados vagos e imprecisos. O Representante da Confederação das Santas Casas e Hospitais Filantrópicos, ponderou que a flexibilização proposta para a comunicação dos dados de saúde deva se dar para “serviços à saúde e de apoio à assistência à saúde, em benefício aos interesses dos titulares”.¹⁹¹

O cruzamento de dados pessoais que envolvem questões atinentes à saúde pode ser parâmetro vital para a ponderação do risco assumido pela seguradora e

¹⁸⁹ CONJUR. **Impactos da LGPD na saúde suplementar e a aprovação de parecer sobre MP 869/2018**. Disponível em: <https://www.conjur.com.br/2019-mai-07/analluza-dallari-impactos-lgpd-saude-suplementar>. Acesso em: 14 jan. 2021.

¹⁹⁰ CONJUR. **Impactos da LGPD na saúde suplementar e a aprovação de parecer sobre MP 869/2018**. Disponível em: <https://www.conjur.com.br/2019-mai-07/analluza-dallari-impactos-lgpd-saude-suplementar>. Acesso em: 14 jan. 2021.

¹⁹¹ *Idem*.

mesmo do valor cobrado ao título de prêmio do seguro ou do plano de saúde. Pela redação dada à Lei Geral de Proteção de Dados Pessoais através da medida provisória número 869, que posteriormente foi convertida na lei ordinária número 13.853, de 8 de julho de 2019, não podem os prestadores de serviços de saúde suplementar valerem-se do cruzamento desses dados para obter vantagem indevida – seja através do aumento do prêmio, seja através da negativa de cobertura securitária. Entretanto, é crível de se pensar que algoritmos possam, ao menos em tese, pelo tratamento desses dados, decidir em nome das seguradoras e dos planos de saúde pelo deferimento ou não da cobertura securitária ou mesmo pelo valor cobrado ao título de prêmio pelo seguro. Segundo a Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização, resultados de diagnósticos, doenças pré-existentes, e, inclusive, condições financeiras são dados que os prestadores de serviços de saúde suplementar almejavam compartilhar¹⁹².

Somado a isso, há o emaranhado de dados capturados a partir dos mecanismos provenientes da *internet* das coisas junto à saúde. Ao tratar sobre o uso da IoT na saúde e a segurança da informação, Meurer enumera uma série de riscos que esses dispositivos podem enfrentar. Os riscos arrolados pelo autor dizem com a falha para fornecer atualizações de *software* de segurança de dispositivos médicos e redes para lidar com vulnerabilidades de dispositivos mais antigos, outro risco pode dizer com a violação da aplicação conectada à IoT por *malwares* que possam alterar os dados do dispositivo, além de distribuição descontrolada de senhas, ou senhas fracas, senhas padrão, e senhas sem validade para expirar¹⁹³.

Buscando mitigar esses problemas, por outro lado, Oliveira e Silva apontam quais são os desafios da IoT na saúde, tendo em vista que o número de dispositivos conectados à *internet* das coisas cresce. Para os autores, “o principal objetivo do IoT na saúde é simplificar a forma como a informação é disponibilizada e aumentar a velocidade com a qual ela pode ser utilizada em prol da saúde do paciente”¹⁹⁴.

¹⁹² *Idem*.

¹⁹³ MEURER, Marciel. **Uso do IoT na saúde e segurança da informação**. 2018. 17 f. Artigo (Especialização) - Curso de Pós-graduação Lato Sensu em Direito, Departamento de Ciências Jurídicas, Universidade do Sul de Santa Catarina, Tubarão, 2018. Disponível em: <https://www.riuni.unisul.br/handle/12345/4942>. Acesso em: 14 jan. 2021. p. 12.

¹⁹⁴ OLIVEIRA, José Lucas Sousa de; SILVA, Rogério Oliveira da. A internet das coisas (IOT) com enfoque na saúde. **Tecnologia em Projeção**, Rio de Janeiro, v. 8, n. 1, p. 77-85, out. 2017. Disponível em: <http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/view/824>. Acesso em: 14 jan. 2021. p. 83.

Conseqüentemente, o principal desafio da *internet* das coisas na saúde é a implementação de padrões de IoT no setor de saúde e sua implementação¹⁹⁵, porque, assim, garantiria um grau de segurança comum entre todos os dispositivos IoT que envolvam dados sensíveis de saúde, e o fato de que “atualização de *firmware*, *hardware* e *software* também precisarão de protocolos de entrega”¹⁹⁶ igualmente para assegurar maior segurança na portabilidade dos dados capturados por essas aplicações.

A sociedade de risco, segundo orientam Silva e Guardia, funciona a partir do que se chama de efeito bumerangue, ou seja, cria-se situações de perigo social que afetam diversas camadas da sociedade¹⁹⁷. Os riscos modernos são formas sistêmicas “de lidar com os perigos e as inseguranças induzidos e introduzidos pelo próprio processo de modernização – pela industrialização tecnológica e pela globalização”¹⁹⁸. Para os autores, em uma releitura de Beck, atualmente há novas formas de risco que são bastante distintas daquelas que existiam antigamente, porque os riscos do passado possuíam causas e efeitos conhecidos, ao passo em que os riscos modernos, em que pese possam deter causa conhecida, possuem hoje conseqüências imprecisas¹⁹⁹. Dessa forma, enquanto os riscos do passado eram unilaterais, os riscos modernos são globais. Para os autores,

na sociedade reflexiva os riscos extrapolam as realidades individuais e até mesmo as fronteiras territoriais e temporais. Produzidos numa região, podem afetar – e continuamente o fazem – outras regiões. Uma nuvem radioativa formada em decorrência de um acidente nuclear, como aconteceu em Chernobyl e, atualmente, em Fukushima, no Japão, não permanece imóvel sobre o local do acidente; a contaminação do mar por mercúrio espalha-se com as correntes marítimas. São riscos que extrapolam também as fronteiras temporais: não apenas a nossa geração está em risco, mas também as gerações futuras estarão. A esse processo dá-se o nome de efeito bumerangue.²⁰⁰

¹⁹⁵ *Idem.*

¹⁹⁶ *Idem.*

¹⁹⁷ SILVA, Roberta Soares da; GUARDIA, Karina Joelma Bacciotti Selingardi. A sociedade de risco global. **Revista de Direito Internacional e Globalização Econômica**, São Paulo, v. 1, n. 1, p. 47-66, out. 2019. Disponível em: <https://revistas.pucsp.br/index.php/DIGE/article/view/42350>. Acesso em: 14 jan. 2021. p. 50.

¹⁹⁸ *Idem.*

¹⁹⁹ SILVA, Roberta Soares da; GUARDIA, Karina Joelma Bacciotti Selingardi. A sociedade de risco global. **Revista de Direito Internacional e Globalização Econômica**, São Paulo, v. 1, n. 1, p. 47-66, out. 2019. Disponível em: <https://revistas.pucsp.br/index.php/DIGE/article/view/42350>. Acesso em: 14 jan. 2021. p. 50.

²⁰⁰ *Idem.*

O efeito bumerangue, quando se trata de *internet* das coisas, não é diferente. Isso porque um incidente de vazamento ou tratamento indevido de dados pessoais, em uma sociedade hiperconectada, é capaz de produzir reflexos nos mais distantes cantos do planeta. A negativa de atendimento nas clínicas e hospitais portugueses, por exemplo, pode servir como exemplo para negativas de cobertura de seguros no Brasil, assim como a utilização de dados de geolocalização na Coreia do Sul serviu como modelo para que grande parte dos países ao redor do globo se valessem da mesma estratégia. A *internet* das coisas, que possui grande potencialidade de capturar dados pessoais, precisa ser trabalhada com maior cuidado por quem produz suas aplicações, minimizando os problemas e propulsionando seus temas. Em nome de maiores facilidades, o mote da IoT, não se pode relevar os riscos abstratos e concretos que o desenvolvimento tecnológico pode causar, especialmente quando se fala sobre dados de saúde.

Nesse sentido, importa refletir sobre quem é o ator responsável pela mitigação dos danos provenientes da má utilização das aplicações conectadas à *internet* das coisas, especialmente quando se trata sobre dados de saúde. Ao discorrer sobre a cibercultura, Pierre Levy aponta que, no desenrolar da história da *world wide web*, foram os próprios cibernautas os responsáveis pelo sucesso da rede mundial de computadores²⁰¹. Para o sociólogo tunisiano, a maioria das grandes transformações técnicas das aplicações conectadas à rede, nos últimos anos, não foi determinada pelas grandes corporações da *internet*. Levy entende que foi o movimento da cibercultura quem fez a *web* tomar o desenvolvimento que tomou, creditando aos internautas o fomento da rede mundial de computadores:

É o movimento social da cibercultura que fez da *Web* o sucesso atual, propagando um dispositivo de comunicação e de representação que correspondia a suas formas de operar e a seus ideais. Os críticos assistem à televisão, que só mostra manchetes espetaculares, enquanto os acontecimentos importantes ocorrem nos processos de inteligência coletiva bastante distribuídos, invisíveis, que escapam necessariamente às mídias clássicas. A *World Wide Web* não foi nem inventada, nem difundida, nem alimentada por macroatores midiáticos como a Microsoft, a IBM, a AT&T ou o exército americano, mas pelos próprios cibernautas.²⁰²

Não se pode crer, todavia, que, sozinhos, os atores do ciberespaço estejam prontos para corrigir os rumos dessa sociedade do risco. É que, se o

²⁰¹ LEVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999. p. 225.

²⁰² LEVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999. p. 225.

desenvolvimento da rede não aconteceu, segundo Levy, em razão dos grandes *players* da sociedade em rede de forma isolada, são essas empresas de tecnologia que, através da *internet* das coisas, buscam o mapeamento e o tratamento desenfreado de dados pessoais. Levy afirma que a tecnologia é produto de uma sociedade e de uma cultura²⁰³. O autor entende que toda técnica é uma produção de uma cultura, e a sociedade se encontra condicionada pelas técnicas que suas culturas produzem²⁰⁴. Ora, se a cultura é quem fecunda a tecnologia, e não sendo os atores do ciberespaço, sozinhos, hábeis a reinventar essa sociedade do risco, resta à legislação tomar as rédeas de quem possui o condão de sobrepor os temas em detrimento dos problemas. Assim, a legislação entra como uma verdadeira atriz para controlar esses riscos trazidos pela modernização.

O cenário da *internet* das coisas e da inteligência artificial trouxe ao ordenamento jurídico novos desafios regulatórios àquele arcabouço que antes existia. É que, frente a essa nova realidade de *big data*, tratamento, compartilhamento e cruzamento de dados pessoais, além da comercialização desses dados como as *commodities* dos tempos modernos, tornou-se inadiável um diálogo sobre a privacidade e sobre as normas que devam nortear esse novo ecossistema. A reflexão, aqui, deve ser “sobre o mundo em que queremos viver e sobre como nos enxergamos nesse novo mundo de dados, decisões algorítmicas e intensificação da relação entre homens e Coisas”²⁰⁵.

No ordenamento jurídico brasileiro, muitas são as fontes que dialogam em busca de uma maior harmonia entre privacidade e humanos, proteção de dados e robôs. A primeira delas, e talvez a mais conhecida, é a Constituição da República Federativa do Brasil, datada de 1988. A Constituição Federal, ainda que de maneira esparsa, tutela o direito à privacidade. Em seu artigo quinto diz-se que a intimidade e a vida privada são direitos invioláveis dentro das fronteiras nacionais²⁰⁶. No ordenamento infraconstitucional, por sua vez, compete ao Código Civil, ao Código de Defesa do Consumidor, ao Marco Civil da Internet e, mais recentemente, à Lei Geral de Proteção de Dados Pessoais a tutela da referida proteção.

²⁰³ *Ibidem*. p. 20.

²⁰⁴ *Ibidem*. p. 50.

²⁰⁵ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p. 55.

²⁰⁶ BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 jan. 2021.

O Código de Defesa do Consumidor, lei federal editada sob o número 8.078, é a legislação brasileira que trata da defesa de todo consumidor no mercado de consumo frente a um fornecedor de serviço ou produto. Como o CDC é a principal norma jurídica protetiva de consumidores frente a fornecedores de produtos ou serviços, por largos anos foi utilizada para assegurar a privacidade e a segurança de consumidores vulneráveis na utilização de aplicações conectadas à *internet* das coisas. É que o CDC traz, na alínea “d” do inciso II de seu artigo quarto, o que se pode chamar de um princípio da Política Nacional das Relações de Consumo. Dito princípio exige uma ação governamental capaz de proteger o consumidor garantindo que produtos e serviços sejam ofertados desde que possuam padrões adequados de segurança, durabilidade, qualidade e desempenho²⁰⁷. Isso quer dizer que, com base no Código de Defesa do Consumidor, “o governo não só está autorizado a intervir para proteger o consumidor, como tem o dever fazê-lo”²⁰⁸.

É que a Política Nacional das Relações de Consumo está envolta em alguns princípios que a ela são norteadores. Esses princípios dizem com a vulnerabilidade, a boa-fé objetiva, e do equilíbrio contratual, aqueles dispostos nos incisos I a VIII do artigo 4º do Código de Defesa do Consumidor. Esses princípios poderiam, em atenção à IoT, ser cumpridos e observados em seu maior grau possível. Isso porque o consumidor de disposições de *internet* das coisas, além da vulnerabilidade contratual que possui, se torna um titular *hiper* vulnerável, haja vista que não possui, via de regra, conhecimento normativo sobre o tema além de sua incompreensão técnica. Também, o inciso II do artigo sexto da legislação consumerista diz ser um direito básico do consumidor, inclusive do consumidor de serviços vinculados à *internet* das coisas, “educação e divulgação sobre o consumo adequado dos produtos e serviços”²⁰⁹. Magrani pondera que esse dispositivo legal “terá grande aplicabilidade à *internet* das coisas”²¹⁰, porque faz com que seja preciso informar aos usuários das aplicações de IoT sobre possíveis riscos que possam ser causados

²⁰⁷ BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Código de Defesa do Consumidor**. Brasília, DF, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 15 jan. 2021.

²⁰⁸ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p. 63.

²⁰⁹ BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Código de Defesa do Consumidor**. Brasília, DF, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 15 jan. 2021.

²¹⁰ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p. 63.

pelo uso dos dispositivos e também sobre as informações que porventura possam ser coletadas através desse uso. Para Magrani, os

inúmeros dispositivos de IoT conectados à internet põem em xeque os direitos de “proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos”, previstos no inciso I do artigo 6º do CDC.²¹¹

Zanata, por sua vez, lembra que, em 2015, um relatório da *Federal Trade Commission* notou que há um grave problema na indústria dos *off-lines*, quando esses passam a fazer parte da cadeia de produtores de tecnologia: não possuem a *expertise* técnica nem os cuidados profissionais de segurança necessários para a proteção dos dados dos usuários de suas aplicações²¹². Por isso, para o Instituto Brasileiro de Defesa do Consumidor, um dos desafios primordiais consistirá no dever de informação adequada e clara sobre os riscos apresentados por um produto ou serviço²¹³. Para Zanata, da mesma forma que existem bulas farmacêuticas com informações sobre riscos causados em determinados medicamentos, “será preciso pensar em formas obrigatórias de comunicação sobre potenciais riscos aos consumidores de dispositivos que integram o universo da *internet das coisas*”²¹⁴.

Outro elemento apostado pelo Código de Defesa do Consumidor é a redação do artigo oitavo da legislação consumerista. O CDC fala que os fornecedores de serviços ou produtos devem se limitar a colocar no mercado tão somente itens cujos riscos sejam normais e previsíveis²¹⁵. Por último, nos artigos 43 e seguintes, o Código de Defesa do Consumidor trata sobre os bancos de dados e cadastros de consumidores, garantindo a esses, os consumidores, acesso aos *big datas* para que tomem conhecimento de fichas e registros e dados pessoais e de consumos individualmente arquivados.

De fato o Código de Defesa do Consumidor se mostrou, por um largo período, como importante ferramenta para o controle da proteção de dados pessoais

²¹¹ *Ibidem*. p. 63-64.

²¹² ZANATTA, Rafael A. F. **Internet das coisas**: privacidade e segurança na perspectiva dos consumidores [contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017]. Brasília: Instituto Brasileiro de Defesa do Consumidor, 2017. p. 5.

²¹³ *Idem*.

²¹⁴ *Idem*.

²¹⁵ BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Código de Defesa do Consumidor**. Brasília, DF, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 15 jan. 2021.

coletados a partir das aplicações vinculadas à *internet* das coisas. Se, pela legislação consumerista, deve haver uma ação governamental capaz de proteger o consumidor garantindo que produtos e serviços sejam ofertados desde que possuam padrões adequados de segurança, durabilidade, qualidade e desempenho, além da necessidade de se minimizar os riscos e elucidar ao consumidor dos potenciais danos que possa estar exposto diante da utilização de dispositivos tecnológicos, parece claro que há uma preocupação legislativa, em um espaço infraconstitucional, com a privacidade e a proteção de dados.

Mais recentemente, contudo, editou-se no Brasil o Marco Civil da *Internet*, outra lei federal, mas, dessa vez, registrada sob o número 12.965. O MCI é a primeira legislação brasileira a exclusivamente destinar-se a tutelar os usuários da rede mundial de computadores. Aprovado em 2014, o Marco Civil da *Internet* prevê garantias, princípios, deveres e direitos para o uso da *web* na Brasil, razão pela qual se pretendeu ser chamado de Constituição da *Internet* no país, porque garantiu diversos princípios e garantias fundamentais em seu corpo legislativo. Nesse sentido, para Fortes, no Marco Civil da *Internet* há previsão expressa sobre dados pessoais, liberdade de expressão liberdade de comunicação e privacidade *on-line*, representando um grande avanço normativo em comparação com o Código de Defesa do Consumidor²¹⁶. No Marco Civil da Internet, a proteção de dados pessoais é tratada de forma específica no seu artigo 10. Lá o legislador tecnológico afirmou que “a guarda e a disponibilização dos registros de conexão e de acesso a aplicações da *internet* [...] bem como de dados pessoais [...] devem atender à preservação da vida privada”²¹⁷. Além disso, Madalena alerta que ainda há riscos de violação da privacidade dos usuários do ciberespaço haja vista que não há previsão, no MCI, de proteção da conexão entre servidor e usuário, o que faz com que seja necessário confiar em criptografia para estabelecer a segurança desses dados²¹⁸, de forma que o acesso a esse *big data* se daria somente a pessoas autorizadas.

Beck lembra que a “promessa de segurança avança com os riscos e precisa ser, diante de uma esfera pública alerta e crítica, continuamente reforçada por meio

²¹⁶ FORTES, Vinicius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet**. Rio de Janeiro: Lumen Juris, 2016. p. 120.

²¹⁷ BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Marco Civil da Internet**. Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 15 jan. 2021.

²¹⁸ MADALENA, Juliano. Comentários ao Marco Civil da internet: lei 12.965, de 23 de abril de 2014. **Revista de Direito do Consumidor**, Brasília, v. 23, n. 94, p. 329-359, ago. 2014. Disponível em: <http://bdjur.stj.jus.br/dspace/handle/2011/77217>. Acesso em: 15 jan. 2021. p. 332.

de intervenções cosméticas ou efetivas no desenvolvimento técnico-econômico”²¹⁹. Assim, ocorre que tanto o Marco Civil da *Internet* quanto o Código de Defesa do Consumidor, em que pese ambos terem suas nuances, não tratam especificamente sobre a proteção de dados pessoais oriundos da saúde. O Marco Civil, mais do que o Código de Defesa do Consumidor, estabelece diretrizes sobre proteção de dados, privacidade e respeito à vida privada na rede mundial de computadores, o que se aplica às conectividades de *internet* das coisas, mas ambas as legislações silenciam quando o assunto é *eHealth*. Também em razão disso, editou-se no Brasil a Lei Geral de Proteção de Dados Pessoais, tombada sob o número 13.709, positivando, de forma expressa, essa categoria de dados pessoais – os vinculados à saúde, conforme se verá oportunamente.

Na sociedade de risco de Beck, portanto, a lei é a atriz, lembrando Levy, responsável por controlar os riscos e balancear temas e problemas. Nessa conjuntura, se a Constituição Federal é vaga ao estabelecer diretrizes sobre a proteção de dados pessoais, o Código de Defesa do Consumidor é genérico sob essa mesma temática, e o Marco Civil da *Internet* não trata sobre dados de saúde coletados na rede, e, aqui, especialmente em aplicações conectadas à *internet* das coisas, cabe à Lei Geral de Proteção de Dados Pessoais realizar essa tarefa. Mas qual é efetivamente a contribuição dada pela LGPD, no Brasil, para tutelar o risco a que estão expostos os usuários de IoT que utilizam ferramentas que capturam dados de saúde? A Lei Geral de Proteção de Dados Pessoais inova em relação a isso? A atuação da LGPD é preventiva à utilização desses dados ou reparadora depois de violada a proteção das informações de saúde? É o que se verá no próximo capítulo.

²¹⁹ BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011. p. 96.

3 AS GERAÇÕES DE NORMAS PROTETIVAS DE DADOS E O CASO BRASILEIRO: COMO A LGPD TRATA OS DADOS PESSOAIS SENSÍVEIS DE SAÚDE COLHIDOS A PARTIR DA INTERNET DAS COISAS?

A proteção de dados pessoais é uma necessidade inerente ao desenvolvimento da *internet* e, conseqüentemente, ao avanço da *internet* das coisas. Quando se trata de dados pessoais de saúde, ou seja, aquela subcategoria de dados pessoais que possam ser considerados sensíveis, elegíveis ao mapeamento do titular dessas informações, essa proteção é ainda mais importante. Em razão disso, no descortinar histórico dos ordenamentos jurídicos, precisamente com nascedouro no continente europeu, leis protetivas de dados pessoais tomaram forma. A principal delas é o Regulamento Geral de Proteção de Dados (RGPR), com jurisdição europeia, por lá resguardando e legislando sobre a matéria.

Esse caminhar das normas protetivas de dados transformou-se com o passar do tempo. Assim, quatro foram as gerações de normas protetivas de dados pessoais, conforme lastreado por Viktor Mayer-Schöenberger e interpretado por Danilo Doneda, até o advento do que se batizou como sendo a quarta geração de normas protetivas de dados pessoais, com a gênese do RGPR. No caso brasileiro, por outro lado, o advento de normas protetivas com o objetivo específico de proteger os dados pessoais se deu com a lei número 13.709, batizada de Lei Geral de Proteção de Dados Pessoais (LGPD). A LGPD, de 14 de agosto de 2018, mas vigente apenas a partir de 2020, enquadrou-se na quarta geração de normas de Mayer-Schöenberger, buscando inovar em relação às leis que, previamente ao seu nascedouro, tutelavam a matéria.

Assim, a tutela dos dados pessoais sensíveis de saúde, por normas protetivas de dados que fazem parte dessa quarta geração, em tese, objetiva prevenir o mau tratamento desses dados colhidos através de aplicações conectadas à *internet* das coisas. Na jurisdição brasileira, por sua vez, novos desafios são empregados à LGPD, ao que, talvez, a forma como a legislação pátria dialoga com os dados pessoais sensíveis não seja a mais bem preparada para essa tarefa preventiva, ocupando papel mais repressor do que moderador. O desafio é a LGPD conseguir ser a atriz necessária para mediar o tema e o problema nessa sociedade de risco. Para compreender isso, precisa-se discorrer sobre a evolução das normas protetivas de dados e pautar a quarta geração de Mayer-Schöenberger.

3.1 PROTEÇÃO DE DADOS E CIBERESPAÇO: O MODELO DE REGULAMENTAÇÃO EUROPEU E O CASO BRASILEIRO

A privacidade e a proteção de dados pessoais, o que também se conhece como *data privacy*, são temas que possuem lugar de fala cada vez mais ativo no meio acadêmico e no Poder Judiciário. Isso porque, desde o surgimento do conceito de privacidade, talvez hoje se esteja diante da maior exposição da imagem humana em sua história. Fato é que, com o desenvolvimento da rede mundial de computadores e dispositivos interconectados virtualmente de forma *on-line*, os dados pessoais transformaram-se no petróleo da atualidade. E, se não bastasse isso, é o próprio usuário do ciberespaço quem concorre com a exposição de seus dados na *internet*.

Em consequência deste novo desafio entabulado à sociedade moderna, ao redor do globo muitos ordenamentos jurídicos se preocuparam em tutelar o direito à privacidade tendo como escopo a proteção de dados pessoais. Nesse sentido, na modernidade, a Europa editou o *General Data Protection Regulation* em 2016 (em que pese o continente europeu tratar legislativamente sobre a matéria desde o século XX), o Uruguai promulgou sua lei protetiva de dados pessoais ainda em 2008, e a Argentina possui leis que defendem a privacidade, neste mesmo enfoque, desde 1994, por exemplo. O Brasil, por último, promoveu sua Lei Geral de Proteção de Dados Pessoais em agosto de 2018, vigente no país desde setembro de 2020. Antes de discorrer sobre a Lei Geral de Proteção de Dados Pessoais brasileira, a fim de concluir sobre a contribuição dada pela LGPD para tutelar o risco a que estão expostos os usuários de IoT que utilizam ferramentas que capturam dados de saúde, importa catalogar o desenvolvimento histórico até o surgimento da LGPD, porque é daí que emanam os traços do que ela se propõe a fazer.

O tratamento normativo depositado na proteção de dados pessoais é cada vez mais presente nos diversos ordenamentos jurídicos ao redor do mundo. Nesse sentido, o respeito aos dados pessoais busca novo e importante papel nas normativas modernas, tendo em vista que está destinada a proteção de dados a mudar determinado “patamar tecnológico e a solucionar previsões pontuais no ordenamento, mas que, em seus desdobramentos, veio a formar as bases para o

que vem sendo tratado, hoje, como um direito fundamental²²⁰ à proteção de dados. Segundo Doneda, a mudança de enfoque dada à proteção de dados pessoais acompanha a classificação evolutiva das leis de proteção de dados²²¹ desenhada por Viktor Mayer-Schöenberger.

Nesse sentido, Mayer-Schöenberger aponta que, na Europa, desde os 1970, a expressão *data protection* tem sido usada como o direito de cada indivíduo em proteger seus próprios dados²²². Em consequência disso, as normas jurídicas que tutelam a proteção de dados pessoais passaram a ser estabelecidas e aceitas como parte do arcabouço legislativo nos países europeus. Como exemplos desses marcos jurídicos de primeira geração tem-se a lei de proteção de dados do estado de Hesse, na Alemanha, datada em 1970, a norma sueca de 1973, a lei de proteção de dados do estado de Rheinland-Pfalz, na Alemanha, de 1974, o *German Bundesdatenschutzgesetz* de 1977.

Tendo em vista esse contexto, o objetivo, segundo narra Mayer-Schöenberger, buscado na criação destes atos foi a proteção de dados em resposta à emergência do processamento de dados por governos e empresas europeus²²³. Isso porque os computadores, que originariamente foram projetados para desvendar códigos e rastrear mísseis, passaram a fazer parte da burocracia estatal²²⁴, tendo em vista que as nações europeias haviam recentemente iniciado massivas reformas sociais e, conseqüentemente, os dados dos cidadãos eram, para Mayer-Schöenberger²²⁵, cada vez mais úteis para o aprimoramento do Estado de bem estar social. Doneda²²⁶, neste sentido, diz que a

primeira dessas quatro gerações de leis era composta por normas que refletiam estado da tecnologia e a visão do jurista à época, pretendendo regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. O núcleo dessas leis

²²⁰ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 22 abr. 2020.

²²¹ *Idem*.

²²² MAYER-SCHÖENBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 220-241.

²²³ *Ibidem*. p. 221.

²²⁴ *Ibidem*. p. 222.

²²⁵ *Ibidem*. p. 222.

²²⁶ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 22 abr. 2020.

girava em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle *a posteriori* por órgãos públicos.

Destaca-se que, à época, sem computadores, um estado de bem estar social moderno não poderia operar. E essa é a explicação dada por Mayer-Schöenberger para justificar a euforia burocrática europeia pelas novas tecnologias. Não apenas governantes, relata o autor, entenderam os benefícios dos computadores, mas também grandes companhias puderam planejar, administrar e gerir melhor seus investimentos. Esse emaranhado de acúmulo de dados, se somado o poder público e a iniciativa privada, fez com que fertilizasse um solo abundoso para propostas gigantescas de centralização de informações²²⁷. Como exemplo tem-se o caso dos computadores instalados para os jogos olímpicos de 1972, na Bavária, onde o estado da Alemanha almejou usá-los para a centralização do Sistema Bávaro de Informações²²⁸. Contudo, se, de um lado, havia a iniciativa privada e o poder público ambos afoitos pelo uso das então novas tecnologias de catalogação e concentração de dados, no outro lado estavam os cidadãos. Mayer-Schöenberger relata que a resistência contra propostas de criação de *databases* aumentava à proporção que o medo dos cidadãos por uma burocracia automatizada e desumanizada se consolidava²²⁹. Assim, os movimentos sociais por proteção de dados tomavam força, expandindo suas fronteiras.

Todavia, conforme pontualmente narra Doneda²³⁰, a falta de experiência com tecnologias ainda pouco familiares ao meio jurídico e legislativo somada ao medo de se autorizar o uso indiscriminado dessas tecnologias, sem que fosse possível medir prováveis e possíveis consequências, fez com que “se optasse por princípios de proteção, não raro bastante abstratos e amplos”²³¹, cujo enfoque básico era a atividade de processamento de dados. Consequentemente, a primeira geração de normas jurídicas sobre a proteção de dados pessoais não possuía como foco a

²²⁷ MAYER-SCHÖENBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 222.

²²⁸ *Idem*.

²²⁹ *Ibidem*. p. 222-223.

²³⁰ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 22 abr. 2020.

²³¹ *Idem*.

proteção da privacidade individual, mas, sim, concentrava sua função no processamento de dados da sociedade²³². E há uma explicação lógica para tanto.

Ora, se, a fim de buscar o bem estar social moderno, era necessário o uso de computadores e de processamento de dados, a legislação europeia, à época, deveria ter como alvo o funcionamento dos computadores e o processamento de dados. Isso porque, se a tecnologia consiste em uma ferramenta poderosa, capaz de trabalhar os dados pessoais das pessoas – o que causou a estranheza da população em geral e o surgimento de movimentos para a edição de leis protetivas de dados –, a tecnologia deve ser usada, segundo diz Mayer-Schöenberger, como um poderoso instrumento de transformação social e política²³³. O uso do processamento de dados, para o autor, precisava ser regulamentado para garantir que estivesse em conformidade com os objetivos da sociedade em geral²³⁴.

A primeira geração de normas protetivas de dados, curiosamente, evitava o uso de termos de fácil compreensão. Mayer-Schöenberger²³⁵ traz, como exemplo, “privacidade”, “informação” e “proteção da vida privada”. Ao invés desses, valia-se de palavras como “dados”, “banco de dados”, “gravação de dados”, “base de dados” e “arquivos de dados”. Acontece que muitos desses conceitos, com o passar do tempo, perderam muito de sua validade²³⁶. Assim, como resultado de sua aplicação, essas leis de proteção de dados de primeira geração “não demoraram muito a se tornar ultrapassadas, diante da multiplicação dos centros de processamento de dados”²³⁷. Por esta razão, como corolário da experiência pessoal dos cidadãos em serem afetados pelo potencial lesivo e irrestrito de processamento de dados, começou-se a requisitar-se direitos sobre a proteção da privacidade individual²³⁸. A necessidade, portanto, de uma nova era legislativa surgiu, dando lugar, assim, para a segunda geração normativa.

²³² MAYER-SCHÖENBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 223.

²³³ *Idem*.

²³⁴ *Idem*.

²³⁵ *Ibidem*. p. 224.

²³⁶ *Ibidem*. p. 225.

²³⁷ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 22 abr. 2020.

²³⁸ MAYER-SCHÖENBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 225.

Por sua vez, a segunda geração de normas protetivas de dados, diferentemente de sua precursora, possuía como característica básica ser fundamentada na vida privada, isto é, sua estrutura “não está mais fixada em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão”²³⁹. Essa evolução (partindo de normas que possuíam como enfoque os computadores para normas que possuíam como foco a privacidade) era reflexo da “insatisfação de cidadãos que sofriam com a utilização por terceiros de seus dados pessoais e careciam de instrumentos para defender diretamente seus interesses”²⁴⁰. E é nesse novo espaço temporal em que direitos como o do esquecimento (*right to be let alone*) voltaram a ser objeto de discussão²⁴¹.

Outrossim, diferentemente das regras de primeira geração, na segunda geração de normas jurídicas protetivas o perigo não se encontrava mais na *surveillance* possivelmente desenvolvida pelos computadores (conforme Mayer-Schöenberger, “o perigo não era mais o *Big Brother*”²⁴²), porque já não havia mais do que poucas bases centralizadas de dados em cada nação²⁴³. A nova realidade, na segunda era das normas jurídicas protetivas de dados, era a pulverização de informações distribuída em milhares de computadores ao redor do mundo, o que, para Mayer-Schöenberger²⁴⁴, fez com que se alterasse o paradigma de busca por proteção de dados.

Assim, nesse novo momento, as normas surgidas não mais se valiam de termos técnicos de difícil assimilação social, mas, sim, de definições mais abstratas e menos conectadas à tecnologia²⁴⁵. Nessa mesma diáspora aos antigos mandamentos, direitos individuais já existentes (como a privacidade, o direito de ser deixado só, o direito ao esquecimento) foram reforçados e conectados aos preceitos

²³⁹ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 22 abr. 2020.

²⁴⁰ *Idem*.

²⁴¹ MAYER-SCHÖENBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 226.

²⁴² Tradução livre de: “The peril was not Big Brother”. *Idem*.

²⁴³ *Idem*.

²⁴⁴ *Idem*.

²⁴⁵ *Idem*.

constitucionais compatíveis²⁴⁶, aumentando sua extensão de subsunção e sua força normativa vinculante. Mayer-Schöenberger ainda traz como exemplo os estatutos francês, austríaco e norueguês.

Importa destacar que, conforme prioriza Doneda, a segunda geração de normas protetivas havia implementado uma sistemática que aportava ao cidadão meios de identificação do uso indevido de seus dados e informações pessoais²⁴⁷. A par do mal uso de seus dados ou informações pessoais, as normas de segunda geração permitiam a propositura de tutela própria pelo usuário violado²⁴⁸. Nas palavras de Mayer-Schöenberger, na

segunda geração de direitos de proteção de dados, os indivíduos obtiveram voz no processo. Seu consentimento às vezes era um pré-requisito para o processamento de dados. Em outros casos, o consentimento individual pode substituir uma presunção legal que proibia o processamento. Esses direitos diferem substancialmente dos direitos de acessar, modificar, e apagar, sob certas condições, os próprios dados pessoais. Os direitos individuais recém-criados delegaram explícito poder de decisão individual para escolher em o que dos seus dados pessoais seria usados e para qual finalidade.²⁴⁹

A proteção de dados, assim, que nasceu para regular a tecnologia, em sua primeira geração, transformou-se em liberdade individual daqueles que pudessem ter sua privacidade exposta. Todavia, se houve uma terceira geração de normas é porque a era que a antecedeu falira. E é a essa medida que Doneda diz que as leis de segunda instância igualmente apresentaram problemas. O autor narra que se percebeu a necessidade de os cidadãos fornecer seus dados pessoais como “um requisito indispensável para a sua efetiva participação social”²⁵⁰. Nesse sentido,

²⁴⁶ MAYER-SCHÖENBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 226.

²⁴⁷ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 23 abr. 2020. p. 97.

²⁴⁸ *Idem*.

²⁴⁹ Tradução livre de: “In the second generation of data-protection rights, individuals obtained a say in the process. Their consent was sometimes a precondition to the data processing; in other instances, individual consent might overwrite a legal presumption that prohibited processing. These rights differed substantially from the rights to access, modify, and under certain conditions delete one’s own personal data. The newly established individual rights delegated explicit decision power to individual to choose what of their personal data would be used for what purposes”. MAYER-SCHÖENBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 227.

²⁵⁰ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 23 abr. 2020. p. 97.

segue o autor ponderando que tanto o Estado quanto os entes privados se valiam dos dados pessoais dos cidadãos para o funcionamento da máquina pública, razão pela qual, se interrompida a transmissão de dados, conseqüentemente por parte de um indivíduo, este seria excluído em algum aspecto de sua vida social²⁵¹.

Já Mayer-Schöenberger²⁵², no mesmo lado, entende que os direitos individuais a serviços sociais e a participação ativa na vida burocrática estatal possuía como requisito básico o contínuo fluxo de transmissão de dados e informações pessoais dos indivíduos. Isso porque, para o autor, cidadãos e sociedade encontram-se intensamente interconectados, o que, se requisitadas eventuais quebras de transmissão de dados, possivelmente acarretaria um custo social muito elevado. Para Mayer-Schöenberger, assim como as viagens e as votações “necessitam dos bancos e do dinheiro, a divulgação de informações pessoais com mais frequência é uma condição prévia para a participação individual”²⁵³.

Na década de 1980 surgiu a terceira geração de leis, que buscou sofisticar a proteção dos dados pessoais, a fim de abranger mais do que a liberdade do cidadão em fornecer ou não suas informações pessoais, mas em efetivamente garantir a liberdade individual daqueles que pudessem ter sua privacidade exposta. Nessa terceira geração de leis, estabelece Doneda, a proteção de dados é vista como um processo complexo, que envolve a “participação do indivíduo na sociedade e considera o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada”²⁵⁴. É nesse momento que surgem as normas jurídicas com previsão legal de autodeterminação informativa.

Portanto, a distinção do caminho histórico das gerações de normas protetivas de dados se mostra bastante acentuado. Isso porque a primeira era de leis dizia com a grande preocupação residir na tutela do direito dos indivíduos ao uso correto dos

²⁵¹ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 23 abr. 2020. p. 97.

²⁵² MAYER-SCHÖENBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 228.

²⁵³ Tradução livre de: “Similarly, from bank and money matters to travel and voting, disclosure of personal information more often than not is a precondition to individual participation”. *Idem*.

²⁵⁴ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 23 abr. 2020. p. 97.

computadores. Isto é, se os computadores existiam, deveriam ser utilizados ao delírio da sociedade, concentrando sua função não nos direitos individuais violados, mas, sim, no processamento de dados. Uma vez que insuficiente para resguardar os cidadãos que possuíssem seus dados violados, porque tão somente se havia legislado sobre o bom uso dos dados pessoais, surgiu a segunda fase de leis. Esta nova geração tornou possível aos indivíduos autorizar ou não o uso de seus dados pessoais, seja por sociedades empresariais, seja pela administração pública. Ocorre que, nessa segunda geração de normas, a requisição de não utilização dessas informações implicava em exclusão social, haja vista que se apontava como vital para a burocracia estatal a utilização e o fluxo contínuo de dados e informações pessoais dos cidadãos. Superada a segunda fase pela terceira era de leis, surge a autodeterminação informativa.

Nesse contexto, autodeterminação informativa significa, ao invés de dizer se um dado ou informação pode ser usado, afirmar *como* um dado ou informação pode ser utilizado. E essa autodeterminação é feita pelo titular do dado ou da informação. O termo autodeterminação informativa foi delineado em 1983 através de uma famosa decisão da Corte Constitucional Alemã. O tribunal alemão foi provocado para que se manifestasse sobre a Lei do Censo (*Volkszählungsgesetz*), que possuía como objetivo, por meio de pesquisa de campo, reunir dados sobre o estágio do crescimento populacional, localização dos habitantes da Alemanha e, dentre outros, a atividade econômica da população²⁵⁵. É que várias foram as demandas provocadas judicialmente pela população alemã, no sentido de que a Lei do Censo “violaria diretamente alguns direitos fundamentais dos reclamantes, sobretudo o direito ao livre desenvolvimento da personalidade”²⁵⁶.

Ao decidir a controvérsia, contudo, o fundamento utilizado pela corte alemã não foi pela inconstitucionalidade da coleta de dados, mas, como afirma Jürgen, pelo “poder do indivíduo, decorrente da ideia de autodeterminação, de decidir em princípio por si próprio, quando e dentro de que limites fatos pessoais serão

²⁵⁵ SCHWABE, Jürgen. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução: Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro, Vivianne Geraldine Ferreira. Montevideo: Fundacion Konrad-Adenauer, 2005. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 23 abr. 2020. p. 233-234.

²⁵⁶ *Ibidem*. p. 234.

revelados”²⁵⁷. E, descrevendo as razões de decidir do tribunal alemão, Jürgen ainda relata que, à época, em 1983, entendia-se naquela jurisdição que

com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas.²⁵⁸

Descrevendo o julgamento, Mayer-Schönenberger lembra que não se tratou de coincidência o surgimento da autodeterminação informativa em um momento em que o direito à liberdade individual da vida privada é reavivado²⁵⁹. Isso porque a decisão alemã, quando entendeu não ser inconstitucional a Lei do Censo, limitou a utilização irrestrita dos dados pessoais consultados. Assim, o Estado alemão poderia tão somente catalogar os dados, mas qualquer tratamento dado a eles deveria ser precedido de consulta a seus titulares. Desta forma, a Corte Constitucional Alemã não apenas vinculou a proteção de dados pessoais como uma previsão constitucional, mas tutelou, através da declaração de necessidade de se consultar o titular dos dados sobre a forma de utilização de suas informações, conforme salienta Jürgen²⁶⁰, a autodeterminação informativa como uma normativa oriunda da norma constitucional alemã.

E, se aplicada como oriunda da norma constitucional alemã, a possibilidade do titular dos dados se autodeterminar informativamente nasceu como uma extensão, uma consequência, um caminho lógico, das liberdades presentes nas leis

²⁵⁷ SCHWABE, Jürgen. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução: Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro, Vivianne Galdes Ferreira. Montevideo: Fundacion Konrad-Adenauer, 2005. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 23 abr. 2020. p. 237.

²⁵⁸ *Idem*.

²⁵⁹ MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 229.

²⁶⁰ SCHWABE, Jürgen. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução: Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro, Vivianne Galdes Ferreira. Montevideo: Fundacion Konrad-Adenauer, 2005. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 23 abr. 2020. p. 238-239.

de segunda geração. A verdade é que a *men legis* das normas de terceira geração alterou significativamente os conceitos já apanhados nas leis de primeira e segunda fases. Doneda descreve, como exemplo da nova ideologia de leis de proteção de dados, calcada na autodeterminação informativa, o tratamento dos dados pessoais visto como um processo, não se encerrando em uma simples permissão para que se use ou não os dados das pessoas, mas, sim, incluindo o titular dos dados “em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender [...] o dever de ser informado”²⁶¹.

Contudo, assim como nas fases anteriores, a terceira era de leis também possuiu suas lacunas. Mayer-Schöenberger descreve que

mesmo quando empoderados com a nova extensão dos direitos individuais, as pessoas não estavam dispostas a pagar o alto preço monetário e os custos sociais que teriam de arcar quando fossem rigorosamente exercitar seu direito à autodeterminação informativa. A esmagadora maioria das pessoas temia o risco financeiro de propor demandas judiciais e temia as circunstâncias e o incômodo das que as ações nos tribunais poderiam causar.²⁶²

Portanto, aponta Doneda, a proteção de dados pessoais, por meio da autodeterminação informativa, era privilégio de poucos²⁶³. Essa minoria, que decidia enfrentar os custos econômicos e sociais para que se exerça o direito de informativamente se autodeterminar, entretanto, não representava a coletividade social que sofria com a frágil segurança de suas informações. E, nesse contexto, em que os legisladores perceberam a posição de negociação fraca dos indivíduos ao exercer seu direito²⁶⁴, uma quarta era se avizinhava.

²⁶¹ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 23 abr. 2020. p. 98.

²⁶² Tradução livre de: “Even when empowered with new and extended participatory rights, people were not willing to pay the high monetary and social cost they would have to expend when rigorously exercising their right of informational self-determination. The overwhelming majority feared the financial risk of filing lawsuits and dreaded the circumstances and the nuisance of court appearances”. MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 232.

²⁶³ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 23 abr. 2020. p. 98.

²⁶⁴ MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 232.

A quarta geração de normas protetivas de dados apontada por Mayer-Schönberger, desde a década de 1990, dividia-se em duas frentes. A primeira delas buscava equalizar a autodeterminação informativa, tendo em vista que almejava preservar a capacidade dos indivíduos em obter proteção a seus dados pessoais reestabelecendo seu empoderamento nas negociações²⁶⁵. Já a segunda delas propunha que os legisladores tomassem parte na liberdade de participação dos cidadãos, entendendo que algumas áreas da privacidade informacional deveriam ser absolutamente protegidas, sem qualquer possibilidade de barganha²⁶⁶.

Desta forma, se em uma mão se procurava em dar mais poder aos indivíduos, outra mão buscava diminuir a força dos Estados e das organizações privadas que porventura detivessem dados pessoais dos usuários. Doneda diz que a quarta geração “surgiu e caracterizou-se por procurar suprir as desvantagens do enfoque individual existente até então”²⁶⁷, procurando-se focar o problema integral da informação, em razão de que “elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção”²⁶⁸. E a principal característica das normas que compõe esta fase é “a disseminação do modelo das autoridades independentes para a atuação da lei”²⁶⁹, como é o caso das legislações vigentes na Argentina, no Uruguai, na União Europeia e, com o advento da Lei Geral de Proteção de Dados Pessoais, no Brasil.

Essa era responde pela atual geração das leis de proteção de dados ao redor do planeta, e mantém o estado da arte de grande parte das normas jurídicas sobre a matéria ao longo do globo. Importa destacar, todavia, que a quarta geração de leis protetivas de dados pessoais veio à tona através da Diretiva 46, editada em 1995 pelo Conselho Europeu (Diretiva 1995/46/CE). A Europa, nesse sentido, sempre esteve na vanguarda das normas protetivas de dados pessoais. Isso porque, afora as normativas interiores de cada Estado do velho continente, a União Europeia, como bloco econômico, desde 1981 exporta normas jurídicas com aplicabilidade a

²⁶⁵ MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997. p. 232.

²⁶⁶ *Ibidem*. p. 233.

²⁶⁷ DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 23 abr. 2020. p. 98.

²⁶⁸ *Idem*.

²⁶⁹ *Idem*.

seus países membros sobre proteção de dados. Essas normas legais, reproduzidas na União Europeia, possuem natureza jurídica distinta, ainda que supraleais, a ponto de terem força vinculante e aplicabilidade em todos os países, incluindo seus cidadãos e as pessoas jurídicas neles domiciliadas, valendo-se como se direito nacional fosse. É o caso dos regulamentos, das convenções, das decisões, das recomendações e das diretivas – como a Diretiva 95/46/CE.

Todavia, antes mesmo da edição da Diretiva 1995/46/CE, em 1995, a Convenção 108, do Conselho Europeu (Convenção 1981/108/CE), também chamada de Convenção de Estrasburgo, inaugurou “as iniciativas para um modelo robusto de tutela, que hoje é referência em todo o mundo”²⁷⁰. A partir da Convenção de Estrasburgo, uma série de normas outras que passaram a compor o ordenamento da Europa de proteção de dados surgiu. A Diretiva 1995/46/CE, por exemplo, é considerada “o texto legal central no sistema europeu de proteção de dados pessoais”²⁷¹. Isso porque, em sua redação contempla os principais conceitos que a proteção de dados pessoais requer. É a Diretiva 1995/46/CE, portanto, quem traz os princípios básicos da tutela de dados, seja na coleta ou na manipulação e tratamento das informações colhidas por interessados ou terceiros. Os direitos básicos de todos os titulares de dados do continente europeu também se encontram discriminados, primeiramente, na Diretiva 1995/46/CE, estabelecendo-se, inclusive, normas que viriam, em 2016, a serem inseridas na Lei Geral de Proteção de Dados Pessoais brasileira, como a transferência internacional de dados e uma autoridade nacional hábil a supervisionar, fiscalizar e arbitrar infrações ao seu texto legal, acarretando em violação de dados pessoais.

Ocorre que, em que pese ser o centro do sistema de proteção de dados europeu, a Diretiva 1995/46/CE não tutela todos os ramos da proteção de dados no continente. Assim, outras diretivas, de caráter complementar, foram também criadas, buscando a transposição do núcleo da Diretiva 1995/46/CE para outras áreas de controle de dados inalcançadas pela norma de 1995. Para Bobbio, um ordenamento jurídico pode ser considerado um sistema não pela impossibilidade de coexistirem

²⁷⁰ GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. **ITS Rio**. Rio de Janeiro, p. 1-24. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 24 abr. 2020. p. 4.

²⁷¹ *Idem*.

normas, mas, sim, pela validade de normas que não são antagônicas entre si²⁷². Nesse contexto, a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho Europeu, foi editada com o objetivo de reger o tratamento conferido aos dados pessoais e a privacidade no setor das comunicações eletrônicas. Segundo Guidi, a norma regulamenta matérias específicas e sensíveis, como, por exemplo, a conservação de “dados de conexão para fins de faturamento dos serviços de conexão prestados, o envio de mensagens eletrônicas não solicitadas (*spam*), a utilização de dados pessoais em listagens públicas (como listas telefônicas), e a utilização dos chamados [...] *cookies*”²⁷³.

Também é caso de legislação extemporânea à Diretiva 1995/46/CE a edição da Diretiva 2006/24/CE, que trabalha especificamente com a *internet*. Nessa diretiva, procurou o Conselho Europeu obrigar os provedores de serviços de comunicação a “reter dados de conexão relativos a comunicações levadas a cabo por meio de redes públicas, com especial menção à *internet*”²⁷⁴. Isso quer dizer que todos os dados produzidos e transmitidos através de redes de conexão *on-line* públicas deveriam ser retidos pelos provedores de *internet*. Contudo, em 2014, através de julgamento proferido pela Corte de Justiça da União Europeia, declarou-se inválida a diretiva, considerando que, mesmo que a retenção de dados não viole os direitos europeus como um todo, a determinação de retenção de todos os dados pessoais transmitidos seria desproporcional²⁷⁵.

Um degrau abaixo das diretivas estão os regulamentos e as decisões. Ambos, os regulamentos e as decisões, possuem força normativa dentro dos Estados membros da União Europeia, razão pela qual compõe o sistema jurídico europeu, com aplicabilidade entre os entes públicos, particulares e privados. Portanto, no que toca aos regulamentos, o Regulamento 2011/45/CE, também do Parlamento Europeu e do Conselho Europeu, foi promulgado tendo como *men legis* do legislador continental tutelar, através de uma norma autoaplicável, vinculando as instituições públicas e privadas e os órgãos da União Europeia, à proteção das pessoas no que

²⁷² BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. 6. ed. Brasília: Editora Universidade de Brasília, 1995. p. 80.

²⁷³ GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. **ITS Rio**. Rio de Janeiro, p. 1-24. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 24 abr. 2020. p. 5.

²⁷⁴ *Idem*.

²⁷⁵ *Idem*.

toca ao respeito ao tratamento de dados por órgãos comunitários, além de a livre circulação desses dados.

Por outro lado, também a fim de complementar as ordens constantes na Diretiva 1995/46/CE, algumas decisões da Comissão Europeia merecem destaque ao ajudar a complementar o quadro regulatório deste modelo de proteção de dados pessoais. Uma das mais famosas decisões da Comissão Europeia é a 2000/520/CE, proferida em 26 de julho de 2000. As razões de decidir diziam sobre a preocupação europeia com o modelo regulatório de proteção de dados estadunidense, tendo em vista que, sendo os Estados Unidos um grande polo empresarial, a exportação de produtos e serviços norte-americanos se apresentava também de forma *on-line*. Portanto, pondera Guidi que “havia a legítima preocupação sobre o destino dos dados de cidadãos europeus eventualmente transferidos a empresas localizadas naquele país”²⁷⁶. Como consequência da Decisão 2000/520/CE, surgiu o programa *Safe Harbor* – ou programa Porto Seguro, em tradução livre.

O programa *Safe Harbor*, em matéria de proteção de dados, nada mais é do que um processo administrativo de auto certificação e cooperação, onde a União Europeia e os Estados Unidos, através da Comissão Europeia e do Departamento de Comércio, respectivamente, comprometeram-se a dar cumprimento às regras de proteção de dados estabelecidas na legislação comunitária da Europa. Desta forma, através do programa *Safe Harbor*, em todas as transações de serviços ou produtos entabuladas do continente europeu e tendo como destino os Estados Unidos, o Departamento de Comércio norte-americano deveria respeitar eventuais normas protetivas de dados vigentes e com aplicabilidade na União Europeia. Dito programa, estabelecido em 2000, operou até o ano de 2015, quando

a Corte de Justiça da União Europeia, diante das denúncias feitas pelo ex-agente da Agência de Segurança Nacional norte-americana (NSA), Edward Snowden, sobre violações generalizadas de privacidade pelo governo estadunidense, julgou inválida a Decisão 2000/520/CE.²⁷⁷

Em consequência ao encerramento do programa *Safe Harbor*, em 2015, novas discussões entre União Europeia e Estados Unidos, sobre segurança de dados no intercâmbio de informações, fez com que a Decisão de Execução

²⁷⁶ GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. **ITS Rio**. Rio de Janeiro, p. 1-24. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 24 abr. 2020. p. 6.

²⁷⁷ *Idem*.

2016/1250/CE, emanada pelo Conselho Europeu, em 2016, desse início ao *Privacy Shield*. Esse novo programa nada mais era do que um aprimoramento do programa Porto Seguro, exigindo que as empresas norte-americanas envolvidas em negócios jurídicos com europeus garantissem o cumprimento de alguns princípios básicos da proteção de dados pessoais, como, por exemplo, o sigilo, a segurança dos dados e a transparência no tratamento dos mesmos.

Apesar de consolidado o sistema europeu de proteção de dados, ainda em 2016 foi aprovada uma grande reforma, iniciada em 2010. Essa reforma se deu, sobretudo, através da inclusão do Regulamento 2016/672/CE, do Parlamento e do Conselho Europeu, substituindo a Diretiva 1995/46/CE e unificando toda a disciplina de proteção de dados pessoais em um único documento. E, através do novo regulamento, implementou-se no modelo europeu de proteção de dados pessoais o *General Data Protection Regulation*.

Também conhecido como GDPR ou RGPD, o regulamento é um ato legislativo da União Europeia que, “pela sua natureza, é parte integrante do direito interno e produz efeito direto simultaneamente nas relações verticais e horizontais, sem necessidade de qualquer mecanismo de recepção”²⁷⁸. Desta forma, assim como as demais normativas anteriormente utilizadas, no âmbito do sistema europeu de proteção de dados pessoais, o GDPR possui aplicabilidade interna nos seus Estados signatários, produzindo efeitos jurídicos tal como se norma interna fosse. Por esta razão o Regulamento Geral de Proteção de Dados prevê um conjunto único de regras consistentes de proteção de dados em toda a União Europeia. A partir do advento, contudo, do GDPR, Guidi aponta sete alterações significativas em comparação com a Diretiva 1995/46/CE.

Entre as principais mudanças trazidas pelo GDPR ao sistema europeu está o reforço aos direitos individuais. O *General Data Protection Regulation* traz previsão expressa no sentido de que o consentimento e a importância do adjetivo “informado” receberam especial atenção. Assim, através do GDPR, exige-se que o titular dos dados pessoais possua acesso “facilitado às informações sobre o tratamento, de modo simplificado [...], e que seu consentimento seja expressado de modo

²⁷⁸ MELO, Ana Sofia Medeiros. **Regulamento Geral de Proteção de Dados: um novo paradigma regulatório**. Orientador: Pedro António Pimenta Costa Gonçalves. 2019. 157 f. Dissertação – Faculdade de Direito da Universidade de Coimbra, Coimbra, 2019. p. 24.

destacado, com igual facilidade para sua revogação”²⁷⁹. O titular dos dados pessoais, assim como futuramente viria a ser previsto na Lei Geral de Proteção de Dados Pessoais brasileira, possui como prerrogativa dar seu consentimento para o uso e o tratamento de seus dados pessoais de forma clara, expressa, e de fácil revogação.

Importa destacar que o acesso ao consentimento, à revogação do consentimento e às informações sobre o tratamento dos dados pessoais, de forma expressa e simplificada, corresponde ao que em 1983 a Corte Constitucional Alemã considerou como sendo a autodeterminação informativa. Portanto, uma vez que a Diretiva 1995/46/CE representava o cerne da quarta geração de normas de proteção de dados pessoais, e se o Regulamento 2016/672/CE passou a ocupar o espaço habitado pela Diretiva, é o *General Data Protection Regulation* o instrumento jurídico nuclear da quarta era de leis protetivas. E assim, por ser a representação europeia da quarta fase de normas jurídicas de proteção aos dados pessoais, possui como ponto fulcral suas bases em uma autoridade independente de proteção de dados pessoais.

Conforme aponta Melo, caso haja eventual violação aos dados pessoais de algum titular no âmbito do sistema europeu, o GDPR “estabelece que os responsáveis pelo tratamento ficam obrigados a notificar as autoridades de proteção de dados”²⁸⁰. Isso porque a competência pela aplicação de eventual sanção aos responsáveis por tratamento de dados que não respeitem as regras do Regulamento é das autoridades de proteção de dados. No modelo europeu, cada Estado membro da União Europeia, ou seja, aqueles cuja subsunção do *General Data Protection Regulation* se faz presente, possui a sua autoridade nacional de proteção de dados. Portanto, são essas autoridades locais que, ao aplicar a norma jurídica do RGPD, fazem valer a proteção de dados pessoais em sua jurisdição.

O Regulamento também prevê diversas regras sobre procedimentos de avaliação de impacto em privacidade, o que Guidi chama de *Privacy Impact*

²⁷⁹ GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. **ITS Rio**. Rio de Janeiro, p. 1-24. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 24 abr. 2020. p. 8.

²⁸⁰ MELO, Ana Sofia Medeiros. **Regulamento Geral de Proteção de Dados: um novo paradigma regulatório**. Orientador: Pedro António Pimenta Costa Gonçalves. 2019. 157 f. Dissertação – Faculdade de Direito da Universidade de Coimbra, Coimbra, 2019. p. 68.

*Assessments*²⁸¹ (ou simplesmente PIAs). Segundo o autor, apesar de “não haver uma obrigação de registro de tratamentos de dados, em certos casos é exigido do controlador ou responsável que elabore tal estudo, de modo a reduzir os riscos à privacidade dos titulares dos dados”²⁸², podendo submetê-lo à aprovação da autoridade nacional de controle competente²⁸³.

Por fim, dentre as alternativas mais relevantes da Diretiva 1995/46/CE para o Regulamento 2016/672/CE, há a inserção de algumas práticas que podem servir como incentivo àqueles responsáveis por eventuais tratamentos de dados pessoais a prezar pelo cumprimento do GDPR e pela garantia da privacidade dos titulares dos dados pessoais. Ditas práticas podem ser concentradas, especialmente, em duas mudanças substanciais: a consolidação dos conceitos de *privacy by default* e *privacy by design*, e a criação de selos de certificação.

Em primeiro lugar, o *General Data Protection Regulation* trouxe a afirmação dos conceitos de *privacy by default* e *privacy by design*. Desta forma, *privacy by default* (ou privacidade padrão) significa que, ao se lançar um produto ou um serviço ao mercado, as configurações de privacidade devem estar pré-estabelecidas da forma mais restrita possível. Isso quer dizer que os consumidores de serviços ou produtos alocados na União Europeia, mesmo que sem capacidade técnica para, com segurança, customizar a restrição de transmissão de seus dados pessoais, possuem como prerrogativa oriunda do GPDR contar com o produto ou serviço previamente editado com as configurações de privacidade no modo mais restritivo possível. Já *privacy by design* é termo desenvolvido nos anos 90 por Cavoukian, para “abordar os efeitos sistêmicos e crescentes das Tecnologias de Informação e Comunicação e sistemas de dados em rede em larga escala”²⁸⁴. O conceito de *privacy by design* significa que em todas as etapas de desenvolvimento de um

²⁸¹ GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. **ITS Rio**. Rio de Janeiro, p. 1-24. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 24 abr. 2020. p. 8.

²⁸² *Idem*.

²⁸³ *Idem*.

²⁸⁴ Tradução livre de: “Privacy by Design is a concept I developed back in the 90’s, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems”. CAVOUKIAN, Ann. **Privacy by design: the 7 foundational principles**. the 7 foundational principles. 2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 24 abr. 2020. p. 1.

produto ou serviço, a privacidade deve ocupar de importância dos programadores²⁸⁵. Isto é, o conceito de privacidade precisa necessariamente estar totalmente inserido no projeto em desenvolvimento, a fim de que se garanta a proteção dos dados pessoais de seus usuários.

Em segundo lugar, a criação de selos e processos de certificação relacionados ao grau de preocupação dada pela empresa prestadora do produto ou fornecedora do serviço no que toca à proteção da privacidade e dos dados pessoais de seus usuários é outra importante medida abarcada pelo GDPR. Sem previsão expressa na Diretriz 1995/46/CE, o Regulamento 2016/672/CE, através da criação dos selos e processos de certificação, regulamentou a escala de proteção de dados pessoais por todo o continente europeu, resguardando ainda mais a privacidade dos titulares dos dados.

A quarta geração das normas protetivas de dados pessoais, portanto, dividia-se em duas grandes frentes: uma que visava à equalização da autodeterminação informativa, ou seja, buscava a manutenção da capacidade de os indivíduos obterem proteção a seus dados pessoais reestabelecendo seu empoderamento nas negociações. Já a segunda frente delas possuía como premissa que os legisladores tomassem parte na liberdade de participação dos cidadãos, entendendo que algumas áreas da privacidade deveriam ser absolutamente protegidas, sem qualquer possibilidade de relativização.

Outro ponto importante que nasceu também no Direito Europeu e, dele, colheu-se inspiração para a LGPD é a tutela jurídica específica sobre os dados pessoais sensíveis, cuja gênese também emerge, em uma norma geral de proteção de dados, na 4ª geração ao abrigo do GDPR. É que a segundo Kokmaz, inspirada na leitura de Rodotá, há uma premissa básica para o surgimento de normas que prevejam tratamento especial aos dados pessoais sensíveis: “é necessária a previsão de normas voltadas a casos específicos referentes à atividade de determinados sujeitos ou à disciplina de categorias específicas de informações”²⁸⁶. O fundamento para a criação de uma categoria autônoma de dados pessoais (e, daí,

²⁸⁵ GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. **ITS Rio**. Rio de Janeiro, p. 1-24. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 24 abr. 2020. p. 8.

²⁸⁶ KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais**: mecanismos de tutela para o livre desenvolvimento da personalidade. 2019. 119 f. Dissertação (Mestrado) – Programa de Pós-graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/11438>. Acesso em: 19 abr. 2021. p. 41.

os dados pessoais sensíveis) se deu a partir da constatação de que o tratamento desses dados poderia acarretar em um risco mais agudo à personalidade dos titulares de dados, ainda mais em se tratando de práticas discriminatórias²⁸⁷. E, em razão disso, o modelo europeu de proteção de dados, materializado no *General Data Protection Regulation*, trouxe consigo essa subcategoria de dados pessoais que, posteriormente, seria abrangida, também, na LGPD brasileira.

Por essa razão, o Regulamento Geral de Proteção de Dados europeu inovou, tornou-se, através de seus dispositivos, o grande espelho para legislações protetivas de dados ao redor do planeta. A ideia do GDPR era, objetivamente, padronizar as normativas de dados europeias, tendo, por ser um regulamento, aplicabilidade em todos os Estados membros. Em razão disso, subterfúgios como *privacy by default* e *privacy by design*, além das certificações de proteção de dados e a previsão de subcategorias de informações protegidas (como a dos dados pessoais sensíveis), foram difundidos em parcela significativa das aplicações que se adequaram à RGPD no continente europeu.

Nesse contexto surge, em 14 de agosto de 2018, a lei número 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais brasileira, que buscou, desde seu nascedouro, ser uma mímica da GDPR em muitas importantes formas²⁸⁸, situando-se na quarta geração histórica de normas protetivas de dados. Segundo Falk,

ainda que se reconheça a estatura constitucional do direito que se pretende tutelar com a LGPD, e mesmo a exigência da edição de lei específica contida no art. 3º, III, da Lei nº 12.956/2014 – considerando que um dos pilares que sustentam o Marco Civil da Internet diz respeito à privacidade dos usuários, na qual estão contidos os dados pessoais por eles produzidos [...] –, é evidente que a exigência europeia de um nível de proteção adequado para a transferência legítima de dados pessoais foi o verdadeiro propulsor da promulgação da lei brasileira, confirme [sic] se verifica,

²⁸⁷ KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**. 2019. 119 f. Dissertação (Mestrado) – Programa de Pós-graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/11438>. Acesso em: 19 abr. 2021. p. 41.

²⁸⁸ ERICKSON, Abigail. Comparative analysis of the EU's GDPR and Brazil's LGPD: enforcement challenges with the LGPD. **Brooklyn Journal of International Law**, Nova Iorque, v. 44, n. 2, p. 859-888, jan. 2019. Disponível em: <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9/>. Acesso em: 18 jan. 2021. p. 859.

extensamente, do voto do então relator da PL, apresentado em 25 de maio de 2018, um dia antes do início da eficácia do Regulamento europeu.²⁸⁹

É que, para o autor, o direito à proteção de dados pessoais apresenta-se como um direito e uma “garantia individual implícita, nos termos do art. 5º, IV, X e XII, da Constituição da República Federativa do Brasil”²⁹⁰. Nessa mesma linha, Doneda afirma que “a Constituição Federal de 1998 ocupa-se do assunto e inclui, entre as garantias e direitos fundamentais de seu artigo 5º, a proteção da intimidade e da vida privada (inciso X), deixando claro que a proteção da pessoa humana abrange este aspecto”²⁹¹. Assim, para Falk, “é inegável o interesse brasileiro na tutela dos dados pessoais, já que sua proteção posiciona-se com corolário do princípio da dignidade da pessoa humana”²⁹². Criticamente, contudo, o motivo pelo qual o Brasil adotou uma legislação protetiva de dados pessoais e se valeu, para tanto, do modelo europeu, antes de ser uma preocupação com a dignidade humana, é, em verdade, uma preocupação comercial, visto que precisava se adequar para fins de realização de contratos.

De toda forma, ter se inspirado no regulamento europeu de proteção de dados pessoais, contudo, não é uma exclusividade brasileira. As propostas de uniformização das diretrizes de proteção de dados pessoais voltam-se a um contexto global, ou seja, maior, onde as normas nacionais, internas a cada jurisdição, não são mais produzidas de maneira desconectada, mas, ainda que confeccionadas dentro de cada país, são redigidas de forma a tratar da proteção de dados pessoais de forma harmônica aos demais Estados. Para Erickson, o tratamento de dados pessoais pelos países está sujeito a um *standard* de regulações, o que pode simplificar um *compliance* para a proteção de dados²⁹³.

Muito em razão dessa cristalina inspiração brasileira no *General Data Protection Regulation*, há uma série de itens comuns entre ambas as legislações.

²⁸⁹ FALK, Matheus. Os “princípios jurídicos” da LGPD e do RGPD: uma leitura a partir da Teoria dos Princípios de Humberto Ávila. *In: WACHOWICZ, Marcos (Org.). Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado.* Curitiba: Gedai, 2020. p. 164.

²⁹⁰ *Ibidem.* p. 163.

²⁹¹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006. p. 107-108.

²⁹² FALK, Matheus. Os “princípios jurídicos” da LGPD e do RGPD: uma leitura a partir da Teoria dos Princípios de Humberto Ávila. *In: WACHOWICZ, Marcos (Org.). Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado.* Curitiba: Gedai, 2020. p. 163.

²⁹³ ERICKSON, Abigail. Comparative analysis of the EU’s GDPR and Brazil’s LGPD: enforcement challenges with the LGPD. *Brooklyn Journal of International Law*, Nova Iorque, v. 44, n. 2, p. 859-888, jan. 2019. Disponível em: <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9/>. Acesso em: 18 jan. 2021. p. 859.

Dentre as principais similitudes entre a LGPD e o GDPR encontram-se as definições dos princípios e das regras contidas nessas normas. É que ambas as normas objetivam a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilidade e prestação de contas no tratamento dos dados pessoais. Seja no artigo quinto da GDPR ou no artigo sexto da LGPD, a segurança e a responsabilidade no uso dos dados pessoais encontram-se estampadas de forma clara. Para Falk, “o instituto da finalidade, presente na LGPD, se coaduna com o da limitação das finalidades previsto pelo RGD²⁹⁴”.

Outro importante ponto de coalisão entre a norma brasileira e o GDPR está no tratamento aos conferido a subcategorias de dados pessoais. É que a “LGPD adotou o modelo europeu para definir o conceito de dado pessoal de uma forma mais ampla²⁹⁵”. Em razão disso, o ordenamento jurídico brasileiro conta, dentre a sua categoria de dados pessoais, com uma em que, assim como a europeia, há, segundo Korkmaz, ampliação das exigências legais com relação ao consentimento do titular dos dados para seu tratamento, ampliação das exigências legais para que se possa realizar o tratamento de determinados tipos de dados pessoais, e aumento de controle e fiscalização no uso de determinados dados pessoais²⁹⁶. Essa subcategoria de dados pessoais é a dos dados pessoais sensíveis, onde se enquadram, conseqüentemente, os dados pessoais de saúde colhidos a partir de aplicações conectadas à *internet* das coisas.

Ocorre que nem sempre a Lei Geral de Proteção de Dados Pessoais brasileira guardou simetria ao Regulamento Geral de Proteção de Dados europeu. A legislação europeia é bastante mais “rígida no tocante à obrigatoriedade da implementação de políticas de governança, proteção de dados e segurança da informação²⁹⁷”. O mesmo se dá quando se trata sobre os direitos da criança e do

²⁹⁴ FALK, Matheus. Os “princípios jurídicos” da LGPD e do RGD: uma leitura a partir da Teoria dos Princípios de Humberto Ávila. *In*: WACHOWICZ, Marcos (Org.). **Proteção de dados pessoais em perspectiva: LGPD e RGD na ótica do direito comparado**. Curitiba: Gedai, 2020. p. 179-180.

²⁹⁵ KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**. 2019. 119 f. Dissertação (Mestrado) – Programa de Pós-graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: <https://repositorio.ufff.br/jspui/handle/ufff/11438>. Acesso em: 19 abr. 2021. p. 60.

²⁹⁶ *Ibidem*. p. 42.

²⁹⁷ SOARES, Rafael Ramos. **Lei Geral de Proteção de Dados – LGPD: direito à privacidade no mundo globalizado**. 2020. 31 f. Monografia (Graduação) – Escola de Direito e Relações

adolescente. A lei número 13.709, de 2018, diz que os menores de 18 anos necessitam de consentimento de ao menos um de seus responsáveis para que possa haver coleta e tratamento de seus dados; a legislação europeia, por sua vez, dá a liberdade de o adolescente de 16 anos em conceder e revogar seu consentimento oportunamente.

Frente a eventuais notificações de violação de dados, isto é, quando há alguma afronta às normas da Lei Geral de Proteção de Dados, não há previsão de prazo, na norma geral protetiva de dados pessoais do Brasil, para que a autoridade competente se manifeste. Isso quer dizer que, administrativamente, necessita-se da utilização de outro marco normativo para que se estabeleça, frente a um diálogo de fontes, qual é o prazo destinado à autoridade competente para que fuja de sua inércia. O que se exige é que o prazo seja minimamente razoável. Quanto ao RGPD, há determinado na norma europeia prazo de 72 horas para a notificação de qualquer incidente cometido a partir da ciência da autoridade competente.

Igualmente há diferenças quanto à responsabilidade pela fiscalização e aplicação de sanções administrativas quando violado algum dos preceitos contidos nas legislações. No caso brasileiro, a Lei Geral de Proteção de Dados Pessoais prevê a existência de uma autoridade nacional de proteção de dados. Dita autoridade, entretanto, segundo Erickson, “está sob o controle do Poder Executivo através da indicação de seus membros pelo Presidente”²⁹⁸. No caso europeu, por outro lado, “a GPDR possui um órgão central, que se chama Comitê Europeu para a Proteção de Dados e é o responsável para a fiscalização e aplicação das sanções e das multas”²⁹⁹. A doutrina, nesse sentido, denuncia que “a LGPD não conseguirá ser efetivamente aplicada com uma autoridade nacional de proteção de dados criada como a que está prevista, sob ordens do Poder Executivo”³⁰⁰. Acontece que, sem

Internacionais, Goiânia, 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1201>. Acesso em: 18 jan. 2021. p. 19.

²⁹⁸ Tradução livre de: “Finally, as created by President Temer’s executive order, the ANPD, is under executive control with board members who are appointed by the President”. ERICKSON, Abigail. Comparative analysis of the EU’s GDPR and Brazil’s LGPD: enforcement challenges with the LGPD. **Brooklyn Journal of International Law**, Nova Iorque, v. 44, n. 2, p. 859-888, jan. 2019. Disponível em: <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9/>. Acesso em: 18 jan. 2021. p. 887.

²⁹⁹ SOARES, Rafael Ramos. **Lei Geral de Proteção de Dados – LGPD: direito à privacidade no mundo globalizado**. 2020. 31 f. Monografia (Graduação) – Escola de Direito e Relações Internacionais, Goiânia, 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1201>. Acesso em: 18 jan. 2021. p. 20.

³⁰⁰ Tradução livre de: “The LGPD cannot be effectively enforced with the ANPD as created by the December 2018 executive order”. ERICKSON, Abigail. Comparative analysis of the EU’s GDPR and Brazil’s LGPD: enforcement challenges with the LGPD. **Brooklyn Journal of International Law**,

uma aplicabilidade efetiva, a Lei Geral de Proteção de Dados não conseguirá, provavelmente, entregar o *compliance* a que se destina. Consequentemente, a falta de aplicabilidade da LGPD acarretará em um difícil diálogo com as demais normas internacionais que tratam da matéria, justamente pela inexistência de uma autoridade nacional de proteção de dados autônoma e independente.

As diferenças entre a LGPD e a GDPR não param por aí. Isso porque, quando se fala sobre dados sensíveis, ainda que na norma estrangeira e legislação brasileira tenha colhido inspiração, a versão europeia de leis protetivas de dados pessoais possui maior detalhamento sobre as categorias especiais de dados pessoais. Como exemplo há a diferenciação entre dados de saúde, dados biométricos e dados genéticos. Já, na versão brasileira, não existe ainda essa distinção categórica, englobando-se todos esses tipos de dados em dados pessoais sensíveis. Somado a isso, não há uma distinção muito específica sobre o que são os dados considerados sensíveis. Consequentemente, “o termo passa a ser subjetivo”³⁰¹.

Segundo Doneda, dados sensíveis seriam “determinados tipos de informação que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva”³⁰². Bioni, por sua vez, diz que os dados sensíveis seriam “uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação”³⁰³. Os dados pessoais sensíveis, dessa forma, são classificados não somente em razão de sua natureza, que é intrinsecamente personalíssima, mas também em decorrência de seu uso. É que, do tratamento de um dado sensível, torna-se capaz de “estabelecer relações e correlações entre os mesmos, permitindo a previsibilidade de condutas, comportamentos, ações, ocorrências e acontecimentos”³⁰⁴.

Nova Iorque, v. 44, n. 2, p. 859-888, jan. 2019. Disponível em: <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9/>. Acesso em: 18 jan. 2021. p. 887.

³⁰¹ COMPUGRAF. **Com a lei em vigor, quais as diferenças entre a LGPD e GDPR?**. Disponível em: <https://www.compugraf.com.br/diferencas-entre-lgpd-e-gdpr/>. Acesso em: 18 jan. 2021.

³⁰² DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 160-161.

³⁰³ BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 14.

³⁰⁴ LEME, Renata Salgado; BLANK, Marcelo. Jurisdição e legislação sanitária comentadas: Lei Geral de Proteção de Dados e segurança da informação na área da saúde. **Cadernos Ibero-americanos de Direito Sanitário**, Brasília, v. 9, n. 3, p. 210-224, jul. 2020. Disponível em:

Nesse sentido, a própria Lei Geral de Proteção de Dados Pessoais, no inciso II de seu artigo quinto, estabeleceu como sendo dado pessoal sensível o “dado pessoal sobre origem racial e étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde [...]”³⁰⁵. Todavia, mesmo frente à insuficiência da Lei Geral de Proteção de Dados pessoais em esmiuçar quais como se trabalha os dados sensíveis, a LGPD foi mais enfática, no cenário nacional, em tratar sobre esse grupo de dados. É que as normas que a preconizaram, ao exemplo da Constituição Federal, do Código de Defesa do Consumidor, e do Marco Civil da Internet, falaram vagamente sobre a proteção de dados pessoais e o direito à privacidade. A LGPD, por outro lado, não só enfrentou a temática como destinou a seção de um capítulo para descortinar a temática.

Uma revolução está em curso crescente na área da saúde e na forma como a Medicina se transformará nos próximos tempos com a aceleração da tecnologia. A *internet* das coisas, conforme apontado no tomo 1.1 deste trabalho, trouxe a tona muitas inovações que auxiliam a busca cada vez mais acentuada pela saúde. Desde *gadgets* e *warables* que se acoplam ao corpo humano mapeando os indicadores clínicos de cada usuário até nano aparelhos de endoscopia, que realizam exames de imagem diminuindo consideravelmente as mazelas de tratamentos agressivos ao corpo humano. A partir da *internet* das coisas na saúde, profissionais habilitados podem elaborar laudos que, em outros tempos, muito mais penosa seria sua confecção. O próprio paciente, em posse de aplicações conectadas à *internet* das coisas, possui condições de mapear sua saúde e, por sua conta, controlar sua vida de modo a garantir-lhe um melhor bem estar.

Por outro lado, se o tema é dados de saúde, o problema é a proteção desses dados. É que essas aplicações conectadas à *internet* das coisas, se têm o condão de garantir benefícios a seus usuários, também captura seus dados pessoais. Esses dados pessoais, que são dados de saúde, são dados pessoais considerados sensíveis pela Lei Geral de Proteção de Dados Pessoais. A LGPD, que se encontra dentro do rol de normas protetivas de dados pessoais pertencentes à quarta geração

<https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/690>. Acesso em: 18 jan. 2021. p. 213.

³⁰⁵ BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 jan. 2021.

de leis protetivas, por um lado busca adequar-se aos preceitos de maior proteção e autonomia ao titular dos dados, mas, por outro, tangencia o direito à proteção de dados de saúde com a mesma importância que trata sua inspiração, o Regulamento Geral de Proteção de Dados europeu.

Nesse sentido, qual é a contribuição dada pela Lei Geral de Proteção de Dados no Brasil para tutelar os riscos a que estão expostos os usuários de aplicações conectadas à *internet* das coisas que utilizam ferramentas que capturam dados pessoais de saúde considerados sensíveis? A Lei Geral de Proteção de Dados Pessoais consegue inovar em relação à Constituição Federal, ao Código de Defesa do Consumidor e ao Marco Civil da Internet e prevenir o mal tratamento dado a essa categoria de dados pessoais, ou a LGPD atua como mecanismo tão somente reparador a essa má utilização? De fato, a lei número 13.709 consegue ser a atriz, lembrando Levy, responsável por balancear tema e problema, bebendo em Beck, nessa sociedade de risco da modernidade? É o que se verá no próximo ponto deste trabalho.

3.2 TUTELA DOS DADOS PESSOAIS SENSÍVEIS DE SAÚDE NA LEI GERAL DE PROTEÇÃO DE DADOS: PREVENÇÃO OU REPARAÇÃO?

A doutrina sociológica, ao longo do tempo, digladiou-se sobre a emergência de uma sociedade de risco, onde os novos tempos poderiam culminar em novos danos, desafios e medos àqueles que enfrentassem essa até então incerta novidade. Dentro desse contexto, a sociedade em rede chegou e consigo trouxe um inabitável universo, potencializando ainda mais aquela antiga sociedade de risco. Assim, os problemas modernos, dentro da rede mundial de computadores, requereram novo posicionamento do Poder Judiciário e, aqui, especialmente do Direito, através do ordenamento jurídico, materializando novas formas de enfrentar e mitigar os riscos daquela nova/velha sociedade.

Esses emergentes desafios oriundos da rede mundial de computadores comportam principalmente os temas que envolvem a proteção de dados pessoais na *web*. É que, de maneira proporcional ao uso da *internet* nas suas mais variadas facetas, o usuário do *ciberespaço* produz dados como se fossem verdadeiras pegadas, deixando tracejados seus passos no mapa da teia. Dos dados pessoais colhidos emana uma série de riscos, tais como o *profiling*, a publicidade dirigida e o

mapeamento de rotinas e interesses dos usuários de aplicações conectadas na *web*. Ocorre que, ao se desenvolver a *internet*, desenvolvem-se também seus perigos. Daí é que o surgimento da *internet* das coisas faz com que os usuários de suas aplicações cada vez mais estejam expostos às problemáticas da grande rede.

IoT, por sua vez, significa a conexão máquina com máquina, isto é, o diálogo inteligente entre dispositivos não naturais, independentemente de interferência e cognição humana. Esses dispositivos, que são dotados de inteligência artificial, pulverizam-se nos setores públicos e privados da sociedade tradicional, particular e comercial. A *internet* das coisas, por exemplo, quando fala sobre sua esfera pública, diz com as cidades inteligentes, a exemplo de Salvador, no estado federado da Bahia, ao utilizar semáforos sensoriais para dinamizar o fluxo do trânsito urbano. No setor privado da *internet* das coisas, a IoT faz com que casas sejam completamente automatizadas, espaços em que torradeiras inteligentes preparam o café da manhã sem que alguém precise, antes, configurar a temperatura dos pães.

Na área da saúde, por outro lado, inúmeros são os exemplos de IoT. A utilização de aplicações conectadas à *internet* das coisas, hoje em dia, na busca por um aprimoramento dos cuidados de saúde de seus usuários, permite que aquele que está em uso das aplicações de IoT possa, por si só, controlar suas métricas clínicas de saúde, ou, ainda, as próprias máquinas virtualmente conectadas são capazes de, sem que haja interferência humana, denunciar previamente potenciais riscos evitando, assim, a ocorrência de algum problema de saúde mais acentuado, conforme já discorrido nesta pesquisa. Esse universo também se apresenta nos hospitais que, ao informatizarem seus prontuários e protocolos, inclusive vinculando-os ao Ministério da Saúde através do e-SUS, compartilhando-os com todas as prefeituras e unidades de saúde públicas, universidades públicas e privadas, permitindo amplo acesso a esses dados por quem possuir manejo da ferramenta governamental, tornaram-se inteligentes ao ponto de induzir tratamentos e condutas à revelia do controle físico realizado por seres humanos. E, por último, curioso exemplo de aplicações de IoT utilizadas para o controle da saúde de seus usuários são aqueles dispositivos que realizam importantes exames de imagem (como a endoscopia) digitalmente, a partir da sensibilidade performativa dos equipamentos, sem a mesma agressão ao organismo que os mesmos exames físicos realizavam.

De um modo geral, a *internet* das coisas é um mecanismo criado para que máquinas, ao dialogarem entre si, tomem decisões ou, quando possível, induzam a

tomada de decisão de humanos usuários de suas aplicações. O objetivo da IoT é trabalhar como facilitadora da vida humana, uma verdadeira assistente artificial de seus consumidores. Nesse sentido, a fim de buscar essas facilitações, a *internet* das coisas transformou-se, dando luz a um novo segmento: a utilização de aplicações conectadas à IoT para fins de saúde. Essa segmentação da IoT diz com, por exemplo, os marca-passos eletrônicos, os exames inteligentes, as aplicações de mapeamento de saúde, tal qual os *gadgets* e *warables* que controlam os indicadores clínicos dos pacientes/usuários. Os dados coletados, nessas aplicações, são mais do que dados pessoais dos usuários, mas dados de saúde, cujo armazenamento, tratamento e compartilhamento requerem especial atenção dos fornecedores de aplicações atreladas à *internet* das coisas.

Em razão disso, uma sociedade que se moldou à interconectividade de dispositivos virtualmente ligados para garantir uma maior comodidade a seus usuários paulatinamente se transformou em uma sociedade de risco, onde a contraprestação a esse comodismo, que é basicamente o tráfego de dados, pode acarretar em graves danos aos usuários de IoT. E, em se tratando de dados de saúde, essa preocupação se potencializa, uma vez que o uso oculto desses dados, que são sensíveis por sua própria natureza, na medida em que aprimora a busca pela saúde física de seus usuários adoece suas privacidades individuais.

Beck defende que os riscos envoltos a uma sociedade, quando normalizados, transformam o contexto social em uma sociedade catastrófica³⁰⁶. Se não bastasse isso, alerta o autor que esse destino civilizatório, da congruência de uma sociedade em uma catástrofe, pode ser potencializado pela modernização³⁰⁷, isto é, pela cibercultura. Levy, por sua vez, sustenta que a cibercultura, isto é, a ciência que nasce a partir do uso da rede mundial de computadores, não se desenvolve exclusivamente a partir dos grandes *players* da *internet*, considerando que foram os próprios cibercultas os responsáveis pelo sucesso da *web*³⁰⁸. Para proteger esses cibercultas, que são os usuários de aplicações conectadas à *internet* das coisas, portanto, o surgimento de leis gerais de proteção de dados emergiu, passando a compor o ordenamento jurídico dos países na figura dos atores responsáveis pela proteção dos titulares de dados pessoais na *internet* e nas aplicações que dela

³⁰⁶ BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011. p. 96.

³⁰⁷ *Idem*.

³⁰⁸ LEVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999. p. 225.

derivam – como, por exemplo, aquelas conectadas à IoT que tratam dados pessoais sensíveis de saúde.

Com o fim de tutelar todo esse universo informacional, o ordenamento jurídico brasileiro viu-se compelido à criação de institutos protetivos de dados pessoais. Essas disposições legislativas começaram a emergir no país através da Constituição da República Federativa do Brasil, de 1988, cujo artigo quinto diz com o direito à privacidade. É bem verdade que existe em tramitação, no parlamento brasileiro, uma proposta de emenda constitucional, que é tombada sob o número 17, do ano de 2019, para que se inclua, no texto da norma constitucional, o direito fundamental à proteção de dados pessoais, o que ainda não ocorreu. Para além da Constituição Federal, outras instituições infraconstitucionais preocuparam-se em legislar sobre a matéria. É o caso, por exemplo, do Código Civil e do Código de Defesa do Consumidor, cujo elo entre fornecedores de serviços e produtos com consumidores fez reverberar diretrizes e obrigações a serem cumpridas para a harmonização das relações de consumo entre os usuários de aplicações conectadas à *internet* das coisas.

Especificamente versando sobre a *internet*, importante fronteira legislativa é o Marco Civil da Internet. Oficialmente instituída sob o número 12.965, do ano de 2014, essa legislação buscou regular o uso da *internet* no Brasil através de princípios, direitos, garantias e obrigações para quem faz uso da rede mundial de computadores. Contudo, ao redor do globo, o movimento legislativo era outro. Enquanto o Brasil tinha vigentes tão somente textos normativos genéricos sobre a atuação dos *ciber* usuários, ao longo da Europa, especialmente, e de alguns países da América Latina o estado da arte das legislações informacionais dizia com ordenamentos específicos sobre a proteção de dados pessoais. É nessa circunstância em que se firma, no corpo legislativo brasileiro, a lei número 13.709, de 14 de agosto de 2018, apadrinhada como Lei Geral de Proteção de Dados Pessoais.

A LGPD surgiu como um verdadeiro bastião às boas práticas de proteção de dados pessoais na *internet*. Seu itinerário possui como finalidade “a proteção dos particulares em relação a seus dados pessoais”³⁰⁹, disciplinando “as atividades

³⁰⁹ MOURA, Marcel Brasil de Souza. As disposições preliminares da LGPD. In: SANTOS, Regiane Martins dos; CARVALHO, Adriana Cristina F. L. (Org.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: OAB, 2020. p. 9.

privada e pública de tratamento de dados pessoais”³¹⁰. É por essa razão que o artigo primeiro da Lei Geral de Proteção de Dados Pessoais diz que a lei dispõe sobre o “tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”³¹¹.

Nesse sentido, a LGPD possui como prerrogativa o tratamento de dados pessoais, sejam eles colhidos de forma analógica ou digital, como aqueles provenientes das aplicações conectadas à *internet* das coisas que armazenam dados pessoais sensíveis de saúde de seus usuários. Esse tratamento de dados poder ser feito por pessoas físicas ou jurídicas, de direito público ou privado. Importa salientar que, para a Lei Geral de Proteção de Dados, mesmo o Estado, quando realiza o tratamento de dados, está pautado pelas balizas de seu corpo normativo. O objetivo da lei, com isso, é justamente proteger os direitos fundamentais de livre desenvolvimento da personalidade, direito à liberdade e à privacidade. A razão disso é que, quando o tratamento de um dado pessoal é realizado de maneira inadequada, compromete-se o desenvolvimento da personalidade, da liberdade e da privacidade do usuário titular daquela informação, justamente porque sua má utilização enerva a formação de práticas danosas, potencializando uma sociedade de risco.

Como consequência de seu objetivo, a LGPD trouxe alguns fundamentos que, correspondendo implicitamente com os preceitos de privacidade da Constituição Federal, exaltaram a proteção de dados pessoais no ordenamento jurídico brasileiro a um novo patamar. Ditos preceitos fundamentais são o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, informação, comunicação e opinião, o desenvolvimento econômico e tecnológico e da inovação, a inviolabilidade da intimidade, honra e imagem, a livre iniciativa, livre concorrência e a defesa consumerista, além dos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania³¹².

³¹⁰ *Idem*.

³¹¹ BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 jan. 2021.

³¹² *Idem*.

A partir do momento em que o legislador trouxe, pela primeira vez, ao ordenamento jurídico brasileiro, a proteção de dados pessoais fundamentada na autodeterminação informativa, fez com que a norma brasileira de proteção de dados pessoais equalizasse-se com a quarta geração das normas protetivas de dados pessoais ao redor do globo. É que essa quarta geração das normas protetivas de dados pessoais, divide-se em duas grandes frentes: uma que visava à dinamização da autodeterminação informativa, ou seja, buscava a manutenção da capacidade de os indivíduos obterem proteção a seus dados pessoais reestabelecendo seu empoderamento nas negociações. Já a segunda frente delas possuía como premissa que os legisladores tomassem parte na liberdade de participação dos cidadãos, entendendo que algumas áreas da privacidade deveriam ser absolutamente protegidas, sem qualquer possibilidade de relativização. Dentre essas subcategorias que necessariamente precisariam ser protegidas há a normatização dos dados pessoais sensíveis, isto é, aqueles cujo uso pode identificar alguém a partir de sua origem racial ou étnica, sua convicção religiosa, opinião política, filiação a organização de caráter religioso, político ou filosófico, ou mesmo a sindicato, dado referente à vida sexual, genético ou biométrico, e, especialmente, os dados de saúde³¹³.

Importa destacar que a quarta geração de normas gerais de proteção de dados pessoais é o que se tem de mais moderno quando o assunto é a proteção de dados. Se o país, portanto, possui uma moderna norma de proteção de dados pessoais, e, diante da emergência do tratamento de dados pessoais de saúde colhidos a partir das aplicações conectadas à *internet* das coisas, espera-se que a LGPD, que possui previsão expressa quanto a subcategoria de dados pessoais sensíveis e, conseqüentemente, portanto, os de saúde, contribua para tutelar o risco a que estão expostos os usuários de IoT que utilizam ferramentas que capturam dados clínicos. O norte dessa proteção, se reparadora ou preventiva, diante do tratamento equivocado desses dados, também é fator determinante para a perfectibilização da norma.

Para se compreender esses temas, algumas conceituações precisam ser esclarecidas. A primeira delas é sobre os dados de saúde. Ora, o tratamento

³¹³ BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 jan. 2021.

dispensado pela Lei Geral de Proteção de Dados Pessoais diverge, em um primeiro momento, no que toca a duas principais categorias de dados. Há os dados comuns, aqueles que são pessoais apenas, e há os dados pessoais sensíveis. Segundo a redação dada ao inciso III do artigo quinto da lei número LGPD, é considerado um dado sensível todo aquele “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”³¹⁴. O que o legislador quer dizer é que todo e qualquer dado pessoal, quando passível sua utilização para a identificação de seu titular, é considerado mais que um dado pessoal, mas um dado pessoal sensível. Nesse sentido, Rodotá diz que

[...] coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como “a proteção de escolhas de vida contra qualquer forma de controle público e estigma social” (L. M. Friedman), como a “reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto” (J. Rosen).³¹⁵

Os dados de saúde, isto é, também aqueles coletados através de aplicações vinculadas a dispositivos atrelados à *internet* das coisas, são considerados dados pessoais sensíveis. Conseqüentemente, por serem considerados dados pessoais sensíveis, seu tratamento diverge se comparado ao tratamento de singelos dados pessoais. Levando-se em consideração o que diz Rodotá, Mulholland pondera que essa principiologia, a da não discriminação, é o ponto fundamental do uso de dados sensíveis potencialmente lesivos³¹⁶. Para a autora, esse princípio da não discriminação é um dos “mais relevantes, no que diz respeito ao tratamento de dados sensíveis”³¹⁷. E segue a autora afirmando que é esse o ponto fundamental “quando diante do uso de dados sensíveis potencialmente lesivo, em decorrência de sua capacidade discriminatória, seja por entes privados - i.e. fornecedoras de

³¹⁴ BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 jan. 2021.

³¹⁵ RODOTÁ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 12.

³¹⁶ MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). **R. Dir. Gar. Fund.**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/download/1603/pdf/>. Acesso em: 02 mar. 2021. p. 166.

³¹⁷ *Idem*.

produtos e serviços – seja por entes públicos”³¹⁸. Pinheiro, nesse sentido, aponta que os dados pessoais sensíveis merecem tratamento especial, porque em determinados contextos a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança “com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais” da pessoa³¹⁹.

A Lei Geral de Proteção de Dados Pessoais brasileira, influenciada pela normativa europeia de proteção de dados, estabelece, em seu artigo 11, as hipóteses onde pode haver o tratamento de dados pessoais sensíveis. É importante referendar que o legislador trouxe um rol taxativo de situações onde somente então seria possível ocorrer o tratamento desses dados. A primeira dessas conjunturas diz com o consentimento. Consentimento, na teoria da proteção de dados, é a autorização que o titular dos dados pessoais dá ao fornecedor de produto ou serviço para que esse, de posse dos dados daquele, possa realizar toda a operação que entender pertinente quanto ao uso desses dados, desde que atendida a sua finalidade específica.

Seguindo a esteira da quarta geração de normas protetivas de dados, Bioni aponta que “o consentimento deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral e, em alguns casos, deve ser, ainda, específico”³²⁰. Isso se justifica, segundo o pesquisador, porque se trata de “uma carga principiológica que procura conformar, justamente, a ideia de que o titular dos dados pessoais deve ser empoderado com o controle de suas informações pessoais e, sobretudo, na sua autonomia da vontade”³²¹. Consequentemente, a LGPD trás, por 35 vezes, a utilização do termo consentimento, a principal base legal para o tratamento de dados pessoais sensíveis.

Isso quer dizer que, sempre que um titular de dados pessoais se valer de aplicações conectadas à *internet* das coisas que capture dados de saúde, que são dados pessoais sensíveis, a regra geral é que a fornecedora do produto e do serviço deverá, antes de realizar o tratamento desses dados, coletar o consentimento desse

³¹⁸ *Idem.*

³¹⁹ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020. p. 63.

³²⁰ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 185.

³²¹ *Ibidem.* p. 186.

titular. Esse consentimento deve ser, obrigatoriamente, claro, específico, livre, inequívoco e informado, ou seja, desacompanhado de qualquer vício que pudesse macular a materialização dessa vontade. E aqui reside a principal problemática que orbita em torno do consentimento. Em nome da autodeterminação informativa, o titular dos dados pessoais não está em paridade de diálogo com o fornecedor do produto e do serviço conectado à *internet* das coisas para expressar seu consentimento, sobretudo em se tratando de dados sensíveis de saúde.

No caso europeu, o GDPR traz essa mesma preocupação. Para o Regulamento Geral de Proteção de Dados do velho continente, em seu artigo nono, o consentimento é particularmente fundamental no tratamento de dados pessoais sensíveis. Para Pinheiro, o que o difere da norma brasileira é que, quando, através do consentimento, o dado pessoal sensível é tornado público, a utilização desse dado pessoal, seu tratamento, independe de qualquer manifestação de vontade do então titular do dado³²². Apesar de se poder questionar e refletir sobre a racionalidade e o poder de barganhar dos titulares de dados pessoais, sobretudo os titulares de dados pessoais sensíveis, para que possam tomar controle efetivo sobre a utilização de seus dados pessoais, o consentimento sempre ocupou lugar de destaque na estratégia regulatória da privacidade informacional.

Bioni, por sua vez, diz que “a sua [do consentimento] adoração pode ser traduzida pelo ciclo de adjetivações recebido ao longo desse trajeto”³²³. O autor aponta que o saldo desse percurso de venerar o consentimento livre, expresso, específico ou inequívoco é uma verdadeira utopia, tendo em vista que aposta no indivíduo como um ser racional, hábil e capaz de controlar suas informações pessoais³²⁴. E isso se justifica porque, muitas vezes, nem mesmo o próprio titular dos dados pessoais consegue compreender quais dados estão sendo coletados e qual é a medida da finalidade do uso desses dados.

Alternativamente, a fim de que se possa garantir o consentimento como um fator que caracterize a liberdade do titular do dado pessoal sensível de saúde em consentir, emerge na doutrina o que se chama de consentimento granular. Korkmaz diz que esse consentimento granular, isto é, o ato de consentir isoladamente para

³²² PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020. p. 63.

³²³ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 188.

³²⁴ *Idem*.

cada tratamento que for feito a cada dado pessoal sensível coletado, permite “uma oxigenação dos processos de tomada de decisão, através do qual a pessoa pode emitir autorizações fragmentadas no tocante ao fluxo de seus dados”³²⁵. Bioni, nesse sentido, aponta que se abre uma margem para que “o controle dos dados seja fatiado de acordo com cada uma das funcionalidades que são ofertadas e se deseja ter e que demandam, respectivamente, tipos diferentes de dados”³²⁶.

O uso do consentimento granular, assim, sendo um consentir fragmentado para cada ato que pudesse ser realizado com cada dado pessoal sensível colhido, serve basicamente para que se possa garantir um consentimento claro, específico, livre, inequívoco e informado, retirando do contexto a hipossuficiência entre o titular dos dados e o desenvolvedor da aplicação de IoT. Em razão disso, o Considerando 43 do GDPR diz que a

fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.³²⁷

Todavia, a LGPD não traz previsão sobre o consentimento granulado, restringindo-se exclusivamente à forma tradicional de consentir. Dessa forma, de acordo com o Considerando 43 da GDPR, esse consentimento em bloco, que não possibilita o ato de consentir “separadamente para diferentes operações de tratamento de dados”³²⁸, não é presumido como uma livre expressão do consentimento. Como consequência disso, a base legal para o tratamento de dados

³²⁵ KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais**: mecanismos de tutela para o livre desenvolvimento da personalidade. 2019. 119 f. Dissertação (Mestrado) – Programa de Pós-graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/11438>. Acesso em: 19 abr. 2021. p. 69.

³²⁶ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 197-198.

³²⁷ UNIÃO EUROPÉIA. Considerando 43 do GDPR, de 25 de maio de 2018. Regulação Geral Sobre a Proteção de Dados. **General Data Protection Regulation**. Disponível em: <https://www.privacy-regulation.eu/pt/r43.htm>. Acesso em: 22 abr. 2021.

³²⁸ *Idem*.

personais, especialmente os dados sensíveis de saúde coletados através de aplicações conectadas à *internet* das coisas, não pode mais se cristalizar simplesmente no consentimento em bloco. Para Binoni:

Tem-se, assim, um quadro regulatório encapsulado por uma compreensão reducionista do conteúdo a que se deve referir autodeterminação informacional que, passadas mais de duas décadas, não mais se ajusta ao contexto subjacente dos dados pessoais como ativo econômico em constante circulação e que modula o livre desenvolvimento da personalidade dos cidadãos.³²⁹

Em razão disso, quando utiliza como base legal para o tratamento de dados pessoais sensíveis o consentimento da forma como prevê, a LGPD não contribui para a mitigação dos riscos a que estão expostos os usuários de IoT, não prevenindo o mal tratamento dos dados de saúde. Ora, se os próprios dados pessoais se tornaram mercadoria, e quem os comercializa é justamente quem os captura, tornando-se um ativo econômico em constante circulação, não há uma paridade de tratamento entre o fornecedor do serviço ou produto e o consumidor. Este é hipossuficiente em relação àquele. É por isso que, nessa circunstância, faz-se necessário reavaliar a estratégia regulatória pautada principalmente no consentimento, verificando “como ser encarado esse descompasso, balanceando soluções que, por um lado, empoderem o titular dos dados pessoais e, por outro lado, não deixem apenas sobre seus ombros a proteção de suas informações pessoais”³³⁰.

Agravando mais a situação, o mesmo artigo 11 da norma jurídica referendada, mas dessa vez em seu inciso II, traz sete novas bases legais específicas que independem do consentimento do titular dos dados pessoais sensíveis. Essas bases legais dizem respeito ao cumprimento de obrigação legal ou regulatória pelo controlador, ao tratamento compartilhado de dados necessário à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, a realização de estudos por órgãos de pesquisa, ao exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, à proteção da vida ou da incolumidade física do titular ou de terceiro, à tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde,

³²⁹ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 188.

³³⁰ *Idem*.

serviços de saúde ou autoridade sanitária, e à garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Sobre a utilização de dados clínicos, dois são os dispositivos legais que chamam maior atenção. As alíneas “e” e “f” do inciso II do artigo 11 da lei número 13.709 apontam que pode ser realizado o tratamento de dados pessoais, independentemente do consentimento dado pelo titular do dado sensível, quando se tratar de “proteção da vida ou da incolumidade física do titular ou de terceiro”³³¹ e “tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”³³². Isso significa que, sempre que o titular dos dados necessitar proteger sua vida ou tutelar sua saúde, seus dados pessoais sensíveis podem ser tratados.

A problemática exsurge pela subjetividade dos termos “proteção da vida” (alínea “e” do inciso II do artigo 11) e “tutela da saúde” (alínea “f” do inciso II do artigo 11). O que são a proteção da vida e a tutela da saúde? Qual é a medida da proteção da vida e qual é a medida da tutela da saúde? E, sendo necessária a utilização desses dados, como será feito esse tratamento? Por quem será feito esse tratamento? São questionamentos que a LGPD não responde, dando uma verdadeira carta branca a quem tiver o condão de *proteger* a vida e *tutelar* a saúde. Mulholland, nesse sentido, entende que o legislador, aprioristicamente, “considera mais relevantes e preponderantes os interesses de natureza pública frente aos interesses do titular”³³³. É que, ao fornecer bases legais vagas, cartas brancas a quem for realizar o tratamento desses dados, intensifica-se a “assimetria de poderes existente entre os titulares de dados e aqueles que realizam o tratamento dos dados”³³⁴. Por outro lado, o parágrafo quarto do artigo 11 da LGPD veda a comunicação e o uso compartilhado desses dados pessoais sensíveis, quando o objetivo é expressamente obter vantagem econômica. Sobre a temática, Gregori

³³¹ BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 jan. 2021.

³³² *Idem*.

³³³ MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). **R. Dir. Gar. Fund., Vitória**, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/download/1603/pdf/>. Acesso em: 02 mar. 2021. p. 168.

³³⁴ *Ibidem*. p. 175.

aponta que duas hipóteses onde a Lei Geral de Proteção de Dados Pessoais autoriza o compartilhamento desses dados:

Especialmente, no tocante à saúde, no § 4º do art. 11, é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: i) a portabilidade de dados quando solicitada pelo titular; ou ii) as transações financeiras e administrativas resultantes do uso e da prestação dos serviços.³³⁵

Nesse ponto, a Lei Geral de Proteção de Dados Pessoais também não protege o titular dos dados pessoais para que seja feito uso estrito desses dados a fins pontuais. A utilização de dados de saúde, em que pese se inibir o compartilhamento econômico desses dados, permite que seja feito o cruzamento dos dados pessoais sem o pretexto de comercialização dessas informações, de forma gratuita. As previsões legais da LGPD não são suficientemente fortes para mitigar os riscos desse cruzamento de dados, permitindo, ainda que de maneira velada, a ocorrência de desvios nesse tratamento de dados pessoais sensíveis de saúde considerando a vagueza de suas cláusulas.

Ainda que não se utilize os dados pessoais sensíveis de saúde colhidos através de disposições conectadas à IoT, é saudável que se reconheça a fragilidade da norma protetiva de dados. Mesmo que editada sob os pilares da proteção da privacidade, da liberdade e do livre desenvolvimento da personalidade da pessoa natural, a redação dada à Lei Geral de Proteção de Dados Pessoais, ao permitir o compartilhamento desses dados, acaba gerando, reflexamente, autorização o cruzamento desses dados, que podem, depois, virem a ser utilizados para fins diversos que não a *tutela* da saúde e a *proteção* da vida. Isso faz com que alguns desafios nasçam dos comandos da Lei Geral de Proteção de Dados Pessoais, a fim de que se garanta a proteção efetiva desses dados pessoais sensíveis, contribuindo para a eficácia da implementação da LGPD aos dados de saúde especialmente colhidos da *internet* das coisas.

³³⁵ GREGORI, Maria Stella. Os impactos da Lei Geral de Proteção de Dados Pessoais na saúde suplementar. **Revista de Direito do Consumidor**, São Paulo, v. 127, n. 29, p. 171-196, jan./fev. 2010. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1268>. Acesso em: 02 mar. 2021. p. 184.

É que, se um dos riscos inerentes ao cruzamento de dados é a montagem de um *profile*, como anteriormente demonstrado, não há dado melhor para tanto do que aqueles considerados sensíveis – e, nesse ponto, os dados de saúde –, porque se prestam justamente para a identificação de seus titulares. E os danos inerentes a essa identificação, o que é típico de uma sociedade do risco, podem ir desde a negativa de prestação de serviços de saúde, como no caso português anteriormente narrado, até mesmo a negativa contratação a empregos, como no caso sul-coreano desenleado alhures. A Lei Geral de Proteção de Dados Pessoais, nesse sentido, não consegue se apresentar como uma verdadeira atriz responsável por balancear tema e problema, bebendo em Beck, naufragando na vagues de suas disposições legais.

Por outro lado, acerta o legislador quando da redação dada ao parágrafo quinto do artigo 11 da Lei Geral de Proteção de Dados Pessoais. Ora, se faz parte do arcabouço de itens relacionados à *internet* das coisas a utilização de *gadgets* que realizem a métrica da frequência cardíaca do usuário, ou do número de vezes em que esse usuário ingere água, ou se realiza atividades físicas, ou mesmo faz parte desse inventário disposições que, ao realizarem um exame de imagem, são capazes de mapear o corpo humano, armazenando um mundaréu de informações, correto é que se vede a utilização desses dados pessoais para, ao menos, dosar risco na contratação de planos privados de assistência à saúde.

Assim, pouca é a contribuição da LGPD no Brasil para tutelar o risco a que estão expostos os usuários de IoT que utilizam ferramentas que capturam dados de saúde. Mesmo que os dados médicos possam ser considerados como valiosas informações sensíveis de saúde, depositadas em aplicações, em hospitais inteligentes, decorrentes de internações e cirurgias, ou mesmo de dispositivos atrelados à IoT, restringiu-se a Lei Geral de Proteção de Dados Pessoais a tutelar, sobretudo, esses dados através do consentimento, uma base legal já ultrapassada, que não reflete a paridade entre usuário e controlador desses dados. Mais além, quando mitiga o uso do consentimento, se vale a LGPD de termos vagos, pouco precisos, que autorizam o uso desses dados independente de uma finalidade pontuada, deixando à margem da interpretação do aplicador a concretude dos dispositivos legais da norma. Já no que diz com o compartilhamento desses dados de saúde, a Lei Geral de Proteção de Dados Pessoais apenas obstaculiza a troca de dados com intuito econômico, deixando aberta qualquer outra transferência de

dados de saúde hábeis a desenhar e identificar o perfil de seu usuário, falhando, portanto, a Lei Geral de Proteção de Dados Pessoais brasileira em seu papel de atriz para o sobrepeso entre tema e problema quando o assunto é a *internet* das coisas e os dados de saúde.

Corroborando com o tema, Oliveira, Gomes, Lopes e Nobre verificam que a LGPD “ao todo possui 65 artigos, que expõe a preocupação com a privacidade dos dados”³³⁶, mas “é possível reduzir casos onde a SI [segurança da informação] acaba sendo negligenciada nos projetos os quais só o simples fato de operar e ser funcional já se mostra um desafio em IoT”³³⁷. Para os autores, a LGPD por si só não consegue destinar-se a proteger os dados pessoais colhidos a partir de aplicações de IoT (e, nesse caso, os dados pessoais sensíveis de saúde também inserem-se nesse diapasão), carecendo de da utilização de técnicas de segurança da informação para “atingir os objetivos da LGPD”³³⁸.

Na medida em que se mostra insuficiente para proteger os dados pessoais, e, principalmente, os dados pessoais sensíveis de saúde, colhidos a partir de aplicações conectadas à *internet* das coisas, porque traz bases legais já ultrapassadas, negligencia o uso de um consentimento granulado, e se vale de expressões cuja vagueza possa se materializar como uma verdadeira carta branca a quem necessitar tratar dados pessoais sensíveis de saúde, violações desses dados porventura ocorrerão. E, ocorrendo alguma violação às diretrizes da LGPD, por sua vez, a norma traz sanções de cunho administrativo que servem tão somente para reparar o dano sofrido, não agindo, pois, a lei como mecanismo preventivo dos riscos a que estão expostos os usuários dessas aplicações de IoT.

Assim, funcionando como uma agente reparadora, prevê a Lei Geral de Proteção de Dados Pessoais advertência, com indicação de prazo para adoção de medidas corretivas aos danos causados, imposição de multa simples ao limite de 2% sobre o faturamento da pessoa jurídica de direito privado agente causadora do dano, limitando-se a cinquenta milhões de reais por infração, multa diária sob o mesmo teto monetário de cinquenta milhões de reais, publicização da infração,

³³⁶ OLIVEIRA, Nairobi Spiecker de; GOMES, Moises Alexandre; LOPES, Ronaldo; NOBRE, Jeferson C.. Segurança da Informação para Internet das Coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD). **Revista Eletrônica de Iniciação Científica em Computação**, Porto Alegre, v. 17, n. 4, p. 1-14, jun. 2019. Disponível em: <https://www.seer.ufrgs.br/reic/article/view/88790/55009>. Acesso em: 01 maio 2020. p. 7.

³³⁷ *Ibidem*. p. 8.

³³⁸ *Idem*.

bloqueio dos dados pessoais a que se refere a infração até a sua regularização, eliminação dos dados pessoais a que se refere a infração, suspensão do funcionamento do banco de dados infrator por no máximo seis meses prorrogáveis por igual período, suspensão do exercício da atividade de tratamento de dados do violador por até seis meses prorrogáveis por igual período e proibição parcial ou total de tratamento de dados e atividades afins do agente violador³³⁹.

Pontualmente, cada uma das infrações narradas no artigo 52 da Lei Geral de Proteção de Dados Pessoais não possui o condão de prevenir a ocorrência de um evento danoso. Ora, a advertência, primeira das infrações disciplinares, com indicação de prazo para adoção de medidas corretivas, somente é aplicada após a ocorrência de alguma infração. Se o próprio dispositivo legal enumera que, junto da advertência, é concedido “prazo para adoção de medidas corretivas”³⁴⁰, é de se colher que justamente o objetivo do legislador é corrigir, isto é, retificar o dano causado pela infração às normas da Lei Geral de Proteção de Dados Pessoais, mas não prevenir a ocorrência de outros eventos danosos.

O mesmo se pode dizer dos demais dispositivos da LGPD. A aplicação de multa diária e de multa simples, por exemplo, ao limite de 2% sobre o faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício financeiro, excluindo-se os tributos, ao limite total de cinquenta milhes de reais por infração, também segue a mesma lógica. Somente haverá a incidência da multa após a ocorrência de um fato danoso proveniente de um agente que maltratou os dados pessoais sensíveis daquele usuário de aplicações conectadas à *internet* das coisas. Antes da ocorrência desse evento não há aplicação de multa. E, mesmo após a ocorrência, o poder da sanção é estritamente recriminador, e não pedagógico, funcionando, também, como uma artimanha repressiva e não preventivamente estrutural. Quando a sanção fala com a publicização da infração cometida após devidamente apurada e confirmada a sua ocorrência, a interpretação possível de ser feita é a de que o legislador busca reprimir o agente causador do dano, desconsiderando, igualmente, àquele que sofrera com o mau uso dos dados pessoais.

³³⁹ BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 jan. 2021.

³⁴⁰ *Idem*.

A LGPD, em casos como esse, para ser mais efetiva na busca pela prevenção da ocorrência de danos, poderia se valer de sanções mais estruturais, cujo objetivo poderia ser a indicação de formas de execução de boas práticas no tratamento de dados pessoais. Ao invés de aplicar uma multa nua e crua, por exemplo, poderia a norma estabelecer outros critérios que, além de reparar o dano sofrido, reestruturassem a própria companhia que violou os dados para que se adequasse às determinações da legislação. Além disso, poderia prever a LGPD a existência de espécies de Considerandos, tal qual o GDPR, com o objetivo de dar ao corpo normativo elementos que induzissem quem está por realizar tratamento de dados pessoais a quais mecanismos de implementação de políticas de boas práticas ou de anonimização de dados, exemplificativamente, possam ser realizados.

De forma preventiva, contudo, na hipótese do inciso V do artigo 52 da lei número 13.709, a lógica inverte-se. É que, ao tratar como sanção administrativa o bloqueio dos dados pessoais a que se refere a infração até a sua regularização, a norma jurídica preocupa-se, principalmente com quem sofrera o dano. É racional de se perquirir que, bloqueando os dados equivocadamente utilizados, até que se apure e regularize a infração cometida, dita infração administrativa funcionaria como uma espécie de tutela de urgência procedimental, evitando-se, isto é, prevenindo-se a persistência do uso daquelas informações até que se solucione o dano sofrido pelo titular dos dados pessoais. O mesmo ocorre na situação do inciso VI do artigo 52 da LGPD, onde a eliminação dos dados pessoais objeto da infração administrativa é solução apontada com o objetivo de prevenir uma reincidência àquele evento danoso.

As hipóteses dos incisos X, XI e XII do artigo 52 da Lei Geral de Proteção de Dados Pessoais dizem respeito à suspensão parcial do funcionamento do banco de dados onde houve o cometimento da infração administrativa, o suspensão do exercício da atividade de tratamento de dados pessoais por aquele que cometeu o ato danoso e proibição, parcial ou total, do exercício de atividades relacionadas com o tratamento de dados pessoais por quem incorreu em erro administrativo em uma má utilização dos dados pessoais. Nessas situações também se busca prevenir, reprimindo, a ocorrência de novos eventos danosos, já que a própria LGPD impede o andamento de novos tratamentos de dados por aqueles que cometeram alguma infração administrativa, mas desde que, primeiro, haja uma infração administrativa.

Dessa forma, a contribuição dada pela Lei Geral de Proteção de Dados Pessoais, no Brasil, para tutelar o risco a que estão expostos os usuários de IoT que utilizam ferramentas que capturam dados de saúde é muito mais reparadora do dano causado do que preventiva propriamente. Fato é que, considerando a subserviência do texto normativo à utilização desses dados, porque há subterfúgios na vagues da norma jurídica que possibilitam o tratamento e o cruzamento dessas informações, o legislador preocupou-se, quando da redação da lei, muito mais em reparar o dano sofrido a prevenir a ocorrência desse mesmo dano.

Pinheiro, ao comentar as sanções previstas na Lei Geral de Proteção de Dados Pessoais, afirma que a LGPD busca estimular que se apliquem os seus dispositivos legais em caráter preventivo, mas que, repressivamente, “a imputação de sanções administrativas faz com que os entes responsáveis pelo tratamento de dados pessoais atentem-se à garantia da segurança das informações que estão utilizando”³⁴¹. Não bastasse isso, o *caput* do artigo 52 da LGPD aponta que a aplicação das sanções, que são de cunho administrativo, restringe-se à atuação de uma autoridade nacional. Isso significa que o titular dos dados, dando-se conta de sua violação, depende da inércia de um ente administrativo que interceda pelo dano sofrido. É bem verdade que é direito do titular dos dados pessoais, conforme o parágrafo primeiro do inciso IX do artigo 18 da LGPD, “peticionar em relação aos seus dados contra o controlador perante a autoridade nacional”³⁴², mas esse ente administrativo, a Autoridade Nacional de Proteção de Dados (ANPD), decota do titular dos dados toda e qualquer ingerência sobre o dano que sofrera. Conforme Pinheiro,

a ANPD tem um papel fundamental como elo entre diversas partes interessadas que vão do titular ao ente privado e ao ente público, passando pela necessidade de alinhamento com demais autoridades reguladoras e fiscalizadoras, bem como os três poderes Executivo, Legislativo e Judiciário que deverão continuar a compreender a temática da dinâmica dos dados pessoais em um contexto não apenas nacional mas principalmente internacional para que o Brasil saiba se posicionar no mercado digital global.³⁴³

³⁴¹ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020. p. 97.

³⁴² BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2021.

³⁴³ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020. p. 30.

Se a quarta geração de normas protetivas de dados pessoais diz com a priorização da autonomia da vontade do titular dos dados pessoais em todas as etapas do processamento de dados, a LGPD falha quando se volta a essa perspectiva na solução de impasses ao mau tratamento desses dados. Antes ainda, a Lei Geral de Proteção de Dados Pessoais brasileira falha ao permitir o tratamento flexibilizado de dados pessoais sensíveis, especialmente aqueles dados de saúde, que são, também, coletados a partir de aplicações conectadas à dispositivos interligados à *internet* das coisas, seja pela imprecisão de seu texto normativo, seja pela sutileza com que possibilita o cruzamento e o compartilhamento desses dados. E, quando violada a norma, as próprias sanções administrativas não buscam prevenir os riscos sofridos, mas tão somente reparar os danos causados.

Com o grande acúmulo de dados oriundos de hospitais inteligentes, exames inteligentes e coisas inteligentes, também grandes são os desafios para adoção, aplicação e manuseio dessas informações. A Lei Geral de Proteção de Dados Pessoais, nesse contexto, ainda que vigente, não inova em relação a suas precursoras, não se posicionando como uma atriz hábil a sopesar tema e problema nessa sociedade de risco moderna, não prevenindo o titular dos dados pessoais em relação aos danos dessa sociedade de risco proveniente da captura de dados por meio da *internet* das coisas, limitando-se a reparar a ocorrência desses eventos danosos, pouco contribuindo, no Brasil, para a tutela dos riscos a que estão expostos os usuários de aplicações conectadas à *internet* das coisas que tem seus dados pessoais sensíveis de saúde tratados.

4 CONCLUSÃO

A evolução da *internet* fez surgir uma nova realidade dentro da rede mundial de computadores. Esse fenômeno foi batizado de *internet* das coisas, isto é, aqueles objetos que, conectados entre si, são capazes de comunicarem-se independentemente da razão humana. A vontade das máquinas, assim, ganhou força e forma, tornando hábeis as coisas a, através de inteligência artificial, induzirem ou tomarem decisões no lugar de seres humanos. Essas coisas conectadas atingiram os mais variados segmentos da industrialização, chegando, inclusive, aos itens de saúde. IoT de saúde, por sua vez, são aqueles aparelhos que buscam trazer maior desenvolvimento saudável aos seus usuários. Nessa esteira encontram-se desde simples *gadgets* e *warables* conectados ao corpo humano até complexos exames médicos que, através da *internet* das coisas, dinamizam os cuidados com a saúde e fazem com que, através de suas facilidades, a vida humana possa ser mais saudável.

Por outro lado, a utilização de aparelhos conectados à *internet* das coisas traz verdadeiras ameaças ao direito à privacidade. A verdade é que a sociedade está preparada para uma guerra, mas não para um ataque de torradeiras, como disse Jarmoc³⁴⁴ em sua rede social *Twitter*. Esses aparelhos inteligentes conectados entre si possuem o condão de, enquanto oferecem facilidades, tomar os dados pessoais dos usuários de IoT. Por essa, vive-se hoje em uma verdadeira sociedade de risco, onde o uso oculto da IoT, e especialmente para fins de saúde, potencializa o surgimento de danos a que os usuários dessas aplicações não estão preparados. Por essa razão, e como consequência dessa sociedade de risco, surgiram as leis gerais protetivas de dados pessoais ao redor do globo e, no caso brasileiro, especificamente a Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, o presente trabalho objetivou responder qual é a contribuição da LGPD no Brasil para tutelar os riscos a que estão expostos os usuários de IoT que utilizam ferramentas que capturam dados de saúde.

Nesse sentido, atendendo aos objetivos específicos do trabalho, o desenvolvimento da *internet* se deu através da oferta pública de acesso à rede

³⁴⁴ JARMOG, Jeff. **In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters**. 21 out. 2016. Twitter: @jjarmoc. Disponível em: <https://twitter.com/jjarmoc/status/789637654711267328>. Acesso em: 25 abr. 2020

mundial de computadores, a *internet* transformou-se em *web*, e a própria *web* passou por algumas metamorfoses. Essas evoluções começaram no que se chamou de *web 1.0*, isto é, a primeira fase da rede. A *read-only-web*, como era conhecida a *web 1.0*, dava conta de que servia rede mundial de computadores exclusivamente para a leitura e formação de cognição. Como consequência, poucas eram as pessoas que poderiam editar conteúdos na rede, servindo a *internet* tão somente como um instrumento de busca, sem a participação da sociedade. Já a segunda geração da *web*, conhecida como *read-write*, permitiu que os usuários da rede a utilizassem de forma mais democrática e plural. Nessa senda, como a *internet* possibilitou a criação de conteúdo de uma forma mais pulverizada, iniciou-se, ali, a produção de dados na rede. A segunda fase da *web* foi suplantada pelas *web 3.0*, *4.0*, *5.0*, o atual estado da arte das redes de dispositivos conectados de forma *on-line*. A terceira fase da *web*, chamada de *web* semântica, possibilitou o surgimento de *softwares* inteligentes, o que viabilizou o desenvolvimento da *internet* das coisas. Assim, elencou-se, em um primeiro momento, a classificação da IoT dentro de um contexto de desenvolvimento da *internet*.

Com o surgimento da *web* semântica, a *internet* das coisas desenvolveu-se. O objetivo da última geração da rede era justamente potencializar a comunicação máquina com máquina, o que acabou ocorrendo precipuamente com a IoT. Esse segmento da rede mundial de computadores, de aplicações inteligentes, que pudessem se comunicar e induzir ou tomar decisões em prol de seus usuários, acabou sendo utilizado nos mais variados segmentos da sociedade. Cidades inteligentes, como Salvador, no estado federado brasileiro da Bahia, informatizaram-se, dinamizando o fluxo de veículos nas ruas a partir de sensores remotos nos semáforos. Carros inteligentes, a exemplo daqueles desenvolvidos pela *player* estadunidense Tesla Inc., tomaram as ruas pilotando de forma autônoma, decidindo pelo momento da frenagem ou pela regulagem da refrigeração interna do veículo, a fim de garantir maior segurança para o motorista e seus passageiros. Livrarias como a *Amazon*, possuidora do *Kindle*, fizeram com que a escolha de livros virtuais fosse mecanizada, com indução de compra a seus usuários a partir de suas preferências literárias. Geladeiras, torradeiras e cafeteiras, dentro das casas das pessoas, e dispositivos de automação como o *Google Home* e a *Amazon Alexa*, fizeram com que o ambiente doméstico encontra-se cada vez mais digital e menos analógico.

Dentro dessa segmentação de disposições conectadas à *internet*, surgiram os dispositivos de IoT atrelados à saúde. Desde *gadgets* e *warables* que se acoplam ao corpo humano mapeando os indicadores clínicos de cada usuário até nano aparelhos de endoscopia, que realizam exames de imagem diminuindo consideravelmente as mazelas de tratamentos agressivos ao corpo humano. A partir da *internet* das coisas na saúde, profissionais habilitados podem elaborar laudos que, em outros tempos, muito mais penosa seria sua confecção. O próprio paciente, em posse de aplicações conectadas à IoT, possui condições de mapear sua saúde e, por sua conta, controlar sua vida de modo a garantir-lhe um melhor bem estar.

Por outro lado, essa sociedade digital, que produz facilitações aos usuários de aplicativos vinculados à IoT, especialmente aqueles dispositivos que tocam à saúde de seus usuários, exige uma contrapartida para a oferta de comodismo. Esse contrapeso atende pela alcunha de dados pessoais, a verdadeira *commoditie* dos novos tempos. A busca por esses dados pessoais é cada vez mais impactante, tendo em vista que sua utilização pode acarretar em um grande negócio para os corporações do mercado negocial. Os dados pessoais, quando tratados, são utilizados desde a formulação e o mapeamento do perfil do titular dos dados até a objetivação de publicidade direcionada, o que é possível desde que se consiga efetuar o tratamento dos dados capturados a partir das mais diversas variantes da IoT. É que o uso oculto dos dados, a destinação não declarada dada ao tratamento dessas informações, fez com que a *internet* das coisas fosse inserida dentro de uma verdadeira sociedade do risco. Quando se trata de dados capturados através de aplicativos de saúde, esses potenciais danos acentuam-se, porque as informações de saúde, que são dados pessoais sensíveis, distinguem-se por possibilitar a identificação do usuário titular desses dados, um verdadeiro prato cheio ao mercado de consumo. Assim, descreveu-se quais são os possíveis danos decorrentes da má utilização de disposições de IoT vinculadas à saúde em uma sociedade do risco.

Em razão disso, a sociedade da facilitação transformou-se morfológicamente, de forma perene, em uma sociedade de risco virtualmente conectada, onde o tema (a facilidade) trouxe consigo um problema (a desproteção de dados pessoais), necessitando de um ator para seu enfrentamento. Esse ator – uma atriz, ao bem da verdade – é a regulamentação da proteção de dados pessoais, conforme se tratou no segundo capítulo dessa dissertação. Para que se pudesse mapear o surgimento das normas protetivas de dados, bem como de suas gerações, ao redor do globo até

o surgimento da LGPD, descreveu-se as quatro grandes fases, onde a primeira delas era composta por normas que refletiam, simploriamente, o estado da tecnologia, regulando um cenário de elaboração de dados e concentração de bancos de dados. Como se mostrava insuficiente, a primeira geração de normas foi superada pela segunda geração, que possuía como característica básica ser fundamentada na vida privada, isto é, sua estrutura se baseava na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão.

Já que também pobre em relação às necessidades da época, a terceira geração de normas surgiu, superando a sua antecessora, e buscando sofisticar os dados pessoais, a fim de abranger mais do que a liberdade do cidadão em fornecer ou não suas informações pessoais, mas em efetivamente garantir a liberdade individual daqueles que pudessem ter sua privacidade exposta. Nessa terceira geração de leis, estabeleceu-se que a proteção de dados era vista como um processo complexo, que envolveria a participação de cada indivíduo titular de dado em um contexto em que lhe fosse solicitado que revelasse seus dados pessoais, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente fosse cerceada. É nesse momento que surgiram as normas jurídicas com previsão legal de autodeterminação informativa. A última fase de normas protetivas, por sua vez, nasceu com o Regulamento Geral de Proteção de Dados (RGPD) europeu, priorizando as autoridades protetivas de dados, e servindo como inspiração para o nascedouro da Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira.

O surgimento de leis protetivas de dados ao redor do globo, portanto, foi um importante contexto para o surgimento da LGPD. Em se tratando de dados de saúde e de *internet* das coisas, essa sociedade da emergência se transforma em uma sociedade do risco, porque, na medida em que são dados pessoais sensíveis os dados de saúde, ou seja, passíveis de identificação de seus usuários, e sendo a IoT verdadeiro vetor de captura e transmissão desses dados, a LGPD surge como uma verdadeira atriz hábil a proteger esses titulares de dados pessoais sensíveis capturados através de disposições conectadas à *internet* das coisas.

Contudo, concluiu-se a investigação, no sentido de que a Lei Geral de Proteção de Dados Pessoais brasileira atua muito mais reprimindo a má utilização dos dados pessoais sensíveis de saúde do que prevenindo essa prática, contribuindo assim para a tutela dos riscos a que estão expostos os usuários de IoT

que utilizam ferramentas que capturam dados de saúde no país. É que a LGPD, ao tratar de dados de saúde, utiliza como base legal primeiramente o consentimento, isto é, autorização dada pelo titular dos dados para o seu uso. Ocorre que esse titular de dados nem sempre se encontra em igual equiparação ao fornecedor dos serviços de IoT de saúde, havendo clara hipossuficiência entre o titular dos dados usuário da aplicação e o fornecedor do dispositivo de *internet* das coisas. Se não bastasse isso, a LGPD traz hipóteses em que pode haver o uso independentemente dessa autorização, mas, ao fazer, discrimina com termos vagos e generalistas essa utilização desconsentida, permitindo sua desvirtuação e não prevenindo a má utilização desses dados. No que toca às sanções pelo mau uso dos dados pessoais sensíveis de saúde, falha a LGPD também, porque busca muito mais inibir a ocorrência de novos riscos a partir do surgimento de algum dano, reprimindo eventual fato danoso já praticado, do que garantindo segurança ao titular dessas informações quanto ao despreocupado tratamento de dados pessoais.

Assim, na verdade, a LGPD não traz consideráveis contribuição para a tutela dos riscos a que estão expostos os usuários de IoT que utilizam ferramentas que capturam dados de saúde, porque se limita a bases legais vagas com terminologias genéricas. O consentimento, que é a principal base legal para tratamento de dados, coloca em disparidade o titular dos dados com o fornecedor da aplicação de IoT, porque muitas vezes nem mesmo o próprio titular dos dados pessoais consegue compreender quais dados estão sendo coletados e qual é a finalidade do uso desses dados para poder, de forma livre, expressa, específica e inequívoca, consentir ou não. Já as demais bases legais removem da esfera do consentimento o uso desses dados pessoais sensíveis de saúde. É que, quando se trata de saúde, a legislação traz expressas previsões onde esses dados podem ser coletados e tratados independentemente da vontade de seu titular. E o mais gravoso é que essas hipóteses de tratamento descompromissado com o consentir são positivadas em termos vagos e genéricos, podendo, por interpretação, serem usadas como subterfúgios para a não utilização da LGPD como um mecanismo de proteção nessa sociedade de risco. Se não bastasse isso, as sanções administrativas previstas na lei, a exemplo da multa, possuem como função preponderantemente a reparação dos danos sofridos, e não a prevenção para a não ocorrência desses danos, reconhecendo-se, assim, uma inglória luta contra essa sociedade de risco.

Essa dissertação não possui o condão de exaurir a matéria aqui abordada, mas, ainda que de uma forma singela, demonstrar como, no campo dos direitos emergentes em uma sociedade global, há problemas práticos e teóricos a serem solucionados que gravitam sob a órbita da temática do trabalho. A Lei Geral de Proteção de Dados Pessoais brasileira surgiu como uma importante ferramenta para consolidar a proteção de dados no país, na esteira da norma europeia e das demais normativas que tratam sobre o assunto ao redor do globo, mas ainda encontra-se dotada de fragilidades, especialmente se tratando de dados pessoais sensíveis, não possuindo, com segurança, força para deter o compartilhamento e o tratamento de dados pessoais de saúde colhidos a partir de aplicações conectadas à IoT, servindo, tão somente, como um instrumento reparador à ocorrência de um dano, e não preventivo à materialização dos dilemas de uma sociedade digitalmente arriscada.

REFERÊNCIAS

AGAMBEN, Giórgio. **Estado de exceção**. São Paulo: Boitempo, 2004.

ALCANTARA, Larissa Kakizaki de. **Big Data e Internet das Coisas**: desafios da privacidade e da proteção de dados no Direito Digital. São Paulo: Independente, 2017.

APÓS novo vazamento de dados, Google antecipa o fim do Google+. Disponível em: <https://info.wsouza.com.br/2018/12/apos-novo-vazamento-de-dados-fim-do-google-plus-e-antecipado.html>. Acesso em: 25 abr. 2020.

ASHTON, Kevin. **That 'Internet of Things' Thing**. 2009. Disponível em: <https://www.rfidjournal.com/articles/view?4986>. Acesso em: 08 jun. 2019.

BBC. **Coronavírus**: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade?. Disponível em: <https://www.bbc.com/portuguese/brasil-52357879>. Acesso em 14 jan. 2021.

BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011.

BERNERS-LEE, Tim. **Weaving the Web**: the original design of the World Wide Web by its inventor. Cambridge: Haper Business, 1999.

BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. 6. ed. Brasília: Editora Universidade de Brasília, 1995.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 jan. 2021.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Marco Civil da Internet**. Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 15 jan. 2021.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 jan. 2021.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Código de Defesa do Consumidor**. Brasília, DF, 11 set. 1990. Disponível em:

http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 15 jan. 2021.

BRISBOURN, Alex. **Tesla's Over-the-Air Fix: best example yet of the internet of things?**. Disponível em: <https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/>. Acesso em: 15 jun. 2019.

CASTELLS, Manuel. **A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. **A Sociedade em Rede: volume 1**. 8. ed. São Paulo: Paz e Terra, 2005.

CAVOUKIAN, Ann. **Privacy by design: the 7 foundational principles**. the 7 foundational principles. 2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 24 abr. 2020.

CISION PR NEWSWIRE. **Takeda and cognition kit presente results from digital wearable technology study in patients with major depressive disorder**. Disponível em: <https://www.prnewswire.com/news-releases/takeda-and-cognition-kit-present-results-from-digital-wearable-technology-study-in-patients-with-major-depressive-disorder-mdd-300558846.html>. Acesso em 17 dez. 2020.

COLOMBO, Silvana; FREITAS, Vladimir Passos de. Da teoria do risco concreto à teoria do risco abstrato na sociedade pós-industrial: um estudo da sua aplicação no âmbito do direito ambiental. **Quaestio Iuris**, Rio de Janeiro, v. 8, n. 3, p. 1895-1912, out. 2015. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/18820>. Acesso em: 13 jan. 2021.

COMPUGRAF. **Com a lei em vigor, quais as diferenças entre a LGPD e GDPR?**. Disponível em: <https://www.compugraf.com.br/diferencas-entre-lgpd-e-gdpr/>. Acesso em: 18 jan. 2021.

CONJUR. **Impactos da LGPD na saúde suplementar e a aprovação de parecer sobre MP 869/2018**. Disponível em: <https://www.conjur.com.br/2019-mai-07/analluza-dallari-impactos-lgpd-saude-suplementar>. Acesso em: 14 jan. 2021.

DATA POINT. Disponível em: <https://whatis.techtarget.com/definition/data-point>. Acesso em 13 jan. 2021.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 2, n. 12, p. 91-108, jul. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 22 abr. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

EFF. **COVID-19 and surveillance tech: year in review 2020**. Disponível em: <https://www.eff.org/pt-br/deeplinks/2020/12/covid-19-and-surveillance-tech-year-review-2020>. Acesso em 14 jan. 2021.

ERICKSON, Abigayle. Comparative analysis of the EU's GDPR and Brazil's LGPD: enforcement challenges with the LGPD. **Brooklyn Journal of International Law**, Nova Iorque, v. 44, n. 2, p. 859-888, jan. 2019. Disponível em: <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9/>. Acesso em: 18 jan. 2021.

ESTADÃO. **Vazamento de senha do Ministério da Saúde expõe dados de 16 milhões de pacientes de COVID**. Disponível em: <https://saude.estadao.com.br/noticias/geral,vazamento-de-senha-do-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid,70003528583>. Acesso em 14 jan. 2021.

EXAME. **Apple se mantém como marca mais valiosa do mundo**. Disponível em: <https://exame.com/tecnologia/apple-se-mantem-como-marca-mais-valiosa-do-mundo-veja-ranking/>. Acesso em 13 jan. 2021.

EXPRESSO. **Clínicas recusaram cuidados a doentes que disseram não ao tratamento de dados pessoais**. Disponível em: <https://expresso.pt/economia/2019-06-08-Clinicas-recusaram-cuidados-a-doentes-que-disseram-nao-ao-tratamento-de-dados-pessoais>. Acesso em 15 jun. 2019.

FALK, Matheus. Os “princípios jurídicos” da LGPD e do RGPD: uma leitura a partir da Teoria dos Princípios de Humberto Ávila. *In*: WACHOWICZ, Marcos (Org.). **Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado**. Curitiba: Gedai, 2020.

FEBRABAN. **Empresas brasileiras perdem quase R\$ 6 mi com vazamento de dados**: Brasil é o país que mais tempo leva para identificar e conter incidentes de segurança, diz estudo global da IBM Security. Disponível em: <https://noomis.febraban.org.br/noomisblog/empresas-brasileiras-perdem-quase-r-6-mi-com-vazamento-de-dados>. Acesso em: 14 jan. 2021.

FORBES. **How IoT is changing the Science of medicine**. Disponível em: <https://www.forbes.com/sites/insights-inteliot/2018/09/14/how-iot-is-changing-the-science-of-medicine/?sh=2e4a79f33e57>. Acesso em 17 dez. 2020.

FORBES. **Tesla supera Toyota como montadora com maior valor de mercado**. Disponível em <https://forbes.com.br/negocios/2020/07/tesla-supera-toyota-como-montadora-com-maior-valor-de-mercado/>. Acesso em 13 jan. 2021.

FORTES, Vinícius Borges; REZER, Morgana Mezalira. Internet das coisas na sociedade de risco: uma análise a partir do direito à privacidade. *In*: CONGRESSO NACIONAL DO CONPEDI, XXVII, 2018, Porto Alegre. **Anais**. Porto Alegre. Disponível em <http://conpedi.danilolr.info/publicacoes/34q12098/91053031/kFt980Gr7fWk908s.pdf>. Acesso em 13 jan. 2021.

FORNASIER, Mateus de Oliveira. The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy. **Rev. Investig. Const.**, Curitiba, v. 6, n. 2, p.297-321, maio 2018. Disponível em: <https://revistas.ufpr.br/rinc/article/view/67592/39878>. Acesso em: 17 abr. 2021.

FORTES, Vinicius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet**. Rio de Janeiro: Lumen Juris, 2016.

FUCHS, Christian et al. Theoretical Foundations of the Web: Cognition, Communication, and Co-Operation. Towards an Understanding of Web 1.0, 2.0, 3.0. **Future Internet**, [S.l.], v. 1, n. 2, p.41-59, fev. 2010. Disponível em: https://www.researchgate.net/publication/41667703_Theoretical_Foundations_of_the_Web_Cognition_Communication_and_Co-Operation_Towards_an_Understanding_of_Web_10_20_30. Acesso em: 11 jun. 2019.

G1. **Operadoras lançam primeira experiência do 5G no Brasil, mas serviço ainda é limitado**. 29 jul. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/07/18/operadoras-lancam-primeira-experiencia-do-5g-no-brasil-mas-servico-ainda-e-limitado.ghtml>. Acesso em: 17 dez. 2020.

GIDDENS, Anthony; BECK, Ulrich; LASH, Scott. **Modernização Reflexiva**. São Paulo: UNESP, 1997. p. 21.

GIL, Henrique Teixeira. A passagem da Web 1.0 para a Web 2.0 e... Web 3.0. **Instituto Politécnico de Castelo Branco: potenciais consequências para uma humanização em contexto educativo**. Castelo Branco, p. 1-2. mar. 2014. Disponível em: <https://repositorio.ipcb.pt/bitstream/10400.11/2404/1/A%20passagem%20da%20Web%20Henrique.pdf>. Acesso em: 22 abr. 2020.

GIVEN IMAGING. **Cápsula endoscópica para endoscopia digestiva**. Disponível em: <https://www.medicalexpo.com/pt/prod/given-imaging/product-75056-720465.html>. Acesso em 17 dez. 2020.

GREENFIELD, Adam. **Everyware: the dawning age of ubiquitous computing**. Berkeley: New Riders, 2006.

GREGORI, Maria Stella. Os impactos da Lei Geral de Proteção de Dados Pessoais na saúde suplementar. **Revista de Direito do Consumidor**, São Paulo, v. 127, n. 29, p. 171-196, jan./fev. 2010. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1268>. Acesso em: 02 mar. 2021.

GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. **ITS Rio**. Rio de Janeiro, p. 1-24. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 24 abr. 2020.

HIGA, Paulo. **De novo**: Yahoo admite outro vazamento, agora com 1 bilhão de contas afetadas. Yahoo admite outro vazamento, agora com 1 bilhão de contas afetadas. 2016. Disponível em: <https://tecnoblog.net/204918/yahoo-vazamento-1-bilhao/>. Acesso em: 25 abr. 2020.

JARMOC, Jeff. **In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters**. 21 out. 2016. Twitter: @jjarmoc. Disponível em: <https://twitter.com/jjarmoc/status/789637654711267328>. Acesso em: 25 abr. 2020.

IBM. **How much would a data breach cost your business?**. Disponível em: <https://www.ibm.com/security/data-breach>. Acesso em: 14 jan. 2021.

IBM. **Monitoring Parkinson's disease with sensors and analytics to improve clinical trials**. 11 abr. 2017. Disponível em: <https://www.ibm.com/blogs/research/2017/04/monitoring-parkinsons-disease/>. Acesso em 17 dez. 2020.

KEEN, Andrew. **The cult of the amateur**: how today's internet is killing our culture. Nova Iorque: Doubleday, 2007.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais**: mecanismos de tutela para o livre desenvolvimento da personalidade. 2019. 119 f. Dissertação (Mestrado) – Programa de Pós-graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/11438>. Acesso em: 19 abr. 2021.

LEME, Renata Salgado; BLANK, Marcelo. Juristição e legislação sanitária comentadas: Lei Geral de Proteção de Dados e segurança da informação na área da saúde. **Cadernos Ibero-americanos de Direito Sanitário**, Brasília, v. 9, n. 3, p. 210-224, jul. 2020. Disponível em: <https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/690>. Acesso em: 18 jan. 2021.

LEMOS, André; BITENCOURT, Elias. Sensibilidade Performativa e Comunicação Das Coisas. **Matrizes**, São Paulo, v. 3, n. 12, p.165-188, set. 2018. Disponível em: <https://www.revistas.usp.br/matrizes/article/download/147528/149830/>. Acesso em: 08 jun. 2019.

LEMOS, André; JESUS, Raniê Solarevisky de. Salvador, cidade inteligente? Comunicação e invisibilidade em experiências de IoT na capital baiana. **Revista Eco-pós**, [S.l.], v. 20, n. 3, p.66-92, 18 dez. 2017. Revista ECO-Pos. <http://dx.doi.org/10.29146/eco-pos.v20i3.14474>.

LEVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

MACHADO, Francisco Muller. **Proposta de protocolo de telemonitoramento sob demanda de sinais biomédicos usando internet das coisas, computação móvel e armazenamento em nuvem**. 2016. 132 f. Dissertação (Mestrado) – Programa de

Pós-graduação em Engenharia Biomédica, Curitiba, 2016. Disponível em: <http://repositorio.utfpr.edu.br:8080/jspui/handle/1/1825>. Acesso em: 17 dez. 2020.

MADALENA, Juliano. Comentários ao Marco Civil da internet: lei 12.965, de 23 de abril de 2014. **Revista de Direito do Consumidor**, Brasília, v. 23, n. 94, p. 329-359, ago. 2014. Disponível em: <http://bdjur.stj.jus.br/dspace/handle/2011/77217>. Acesso em: 15 jan. 2021.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018.

MARTINS, Joana Castel-Branco Saldanha. **A Internet das Coisas em Serviços de Saúde**. 137 f. Dissertação (Mestrado) – Faculdade de Economia e Gestão, Universidade Católica Portuguesa, Porto, 2019. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/28405/1/TFM_JoanaSaldanha.pdf. Acesso em: 17 dez. 2020.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997.

MELO, Ana Sofia Medeiros. **Regulamento Geral de Proteção de Dados: um novo paradigma regulatório**. Orientador: Pedro António Pimenta Costa Gonçalves. 2019. 157 f. Dissertação – Faculdade de Direito da Universidade de Coimbra, Coimbra, 2019.

MEURER, Marciel. **Uso do IoT na saúde e segurança da informação**. 2018. 17 f. Artigo (Especialização) - Curso de Pós-graduação Lato Sensu em Direito, Departamento de Ciências Jurídicas, Universidade do Sul de Santa Catarina, Tubarão, 2018. Disponível em: <https://www.riuni.unisul.br/handle/12345/4942>. Acesso em: 14 jan. 2021.

MORAIS, José Luis Bolzan de. O Estado de Direito como mecanismo político-jurídico do liberalismo. In: MORAIS, José Luis Bolzan de; LOBO, Edilene (Orgs.). **Temas de Estado de Direito e Tecnologia**. Porto Alegre: Editora Fi, 2001.

MORCH. **IoT na Medicina: 9 Exemplos de como a Internet das Coisas avança na saúde**. 29 abr. 2019. Disponível em: <https://telemedicinamorsch.com.br/blog/iot-na-medicina>. Acesso em: 17 dez. 2020.

MOURA, Marcel Brasil de Souza. As disposições preliminares da LGPD. In: SANTOS, Regiane Martins dos; CARVALHO, Adriana Cristina França Leite de. (Org.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: OAB, 2020.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). **R. Dir. Gar. Fund.**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em:

<https://sisbib.emnuvens.com.br/direitosegarantias/article/download/1603/pdf/>. Acesso em: 02 mar. 2021.

NAIK, Umesha; SHIVALINGAIAH, D. Comparative Study of Web 1.0, Web 2.0 and Web 3.0. In: 6° INTERNATIONAL CALIBER, 6., 2008, Allahabad. **Anais 6° International CALIBER**. Allahabad: Inflibnet Centre, 2008. v. 1, p. 499-507. Disponível em: <https://ir.inflibnet.ac.in/bitstream/1944/1285/1/54.pdf>. Acesso em: 22 abr. 2020.

NASCIMENTO, Rodrigo. **O que, de fato, é internet das coisas e que revolução ela pode trazer?**: a resposta saberemos nos próximos anos, mas uma coisa é certa, uma nova revolução digital está prestes a acontecer. 2015. Disponível em: <https://computerworld.com.br/2015/03/12/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer/>. Acesso em: 08 jun. 2019.

O GLOBO. **Apple e Hyundai vão se unir para construir carro elétrico autônomo**. Disponível em: <https://oglobo.globo.com/economia/apple-hyundai-vao-se-unir-para-construir-carro-eletrico-autonomo-24831844>. Acesso em 13 jan. 2021.

OLHAR DIGITAL. **Como governos estão usando dados de localização dos celulares no combate à Covid-19**. Disponível em: <https://olhardigital.com.br/2020/03/28/noticias/como-governos-estao-usando-dados-de-localizacao-dos-celulares-no-combate-a-covid-19/>. Acesso em 14 jan. 2021.

OLIVEIRA, José Lucas Sousa de; SILVA, Rogério Oliveira da. A internet das coisas (IOT) com enfoque na saúde. **Tecnologia em Projeção**, Rio de Janeiro, v. 8, n. 1, p. 77-85, out. 2017. Disponível em: <http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/view/824>. Acesso em: 14 jan. 2021.

OLIVEIRA, Nairobi Spiecker de; GOMES, Moises Alexandre; LOPES, Ronaldo; NOBRE, Jeferson C.. Segurança da Informação para Internet das Coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD). **Revista Eletrônica de Iniciação Científica em Computação**, Porto Alegre, v. 17, n. 4, p. 1-14, jun. 2019. Disponível em: <https://www.seer.ufrgs.br/reic/article/view/88790/55009>. Acesso em: 01 maio 2020.

PASQUALE, Frank. **The Black Box Society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

PRIVACY TECH. **Mais de 200 milhões de brasileiros têm dados pessoais expostos em nova falha de segurança do Ministério da Saúde**. Disponível em: <https://privacytech.com.br/destaque/mais-de-200-milhoes-de-brasileiros-tem-dados-pessoais-expostos-em-nova-falha-de-seguranca-do-ministerio-da-saude.,381645.jhtml>. Acesso em 14 jan. 2021.

PRIVACY TECH. **Vazamento no Ministério da Saúde expõe dados de 16 milhões de pacientes de COVID.** Disponível em:

<https://privacytech.com.br/destaque/vazamento-no-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid.381009.jhtml>. Acesso em 14 jan. 2021.

PURDY, Mark; DAVARZANI, Ladan; OVANESSOFF, Armen. **Como a Internet das Coisas Pode Levar à Próxima Onda de Crescimento no Brasil.** 2015. Disponível em: <https://hbrbr.uol.com.br/como-a-internet-das-coisas-pode-levar-a-proxima-onda-de-crescimento-no-brasil/>. Acesso em: 15 jun. 2019.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: privacidade hoje.** Rio de Janeiro: Renovar, 2008.

SANGOI, Rafael Martins. **A Necessidade de Adaptação do Direito ao Tempo da Internet: desafios e perspectivas para a cidadania digital contemporânea.** 2019. 120 f. Dissertação (Mestrado) - Curso de Programa de Pós-graduação Stricto Sensu em Direito, Departamento de Ciências Sociais Aplicadas, Universidade Regional Integrada do Alto Uruguai e das Missões, Santo Ângelo, 2019.

SANTOS, Pedro Miguel Pereira. **Internet das coisas: o desafio da privacidade.** 2016. 108 f. Dissertação (Mestrado) - Curso de Sistemas de Informação Organizadas, Instituto Politécnico de Setúbal, Setúbal, 2016. Disponível em: <http://comum.rcaap.pt/bitstream/10400.26/17545/1/Disserta%c3%a7%c3%a3o%20Pedro%20Santos%20140313004%20MSIO.pdf>. Acesso em: 01 maio 2020.

SCHWABE, Jürgen. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.** Tradução: Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro, Vivianne Gerales Ferreira. Montevideo: Fundacion Konrad-Adenauer, 2005. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 23 abr. 2020.

SILVA, Roberta Soares da; GUARDIA, Karina Joelma Bacciotti Selingardi. A sociedade de risco global. **Revista de Direito Internacional e Globalização Econômica**, São Paulo, v. 1, n. 1, p. 47-66, out. 2019. Disponível em: <https://revistas.pucsp.br/index.php/DIGE/article/view/42350>. Acesso em: 14 jan. 2021.

SOARES, Rafael Ramos. **Lei Geral de Proteção de Dados – LGPD: direito à privacidade no mundo globalizado.** 2020. 31 f. Monografia (Graduação) – Escola de Direito e Relações Internacionais, Goiânia, 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1201>. Acesso em: 18 jan. 2021.

THE WASHINGTON POST. **A ‘travel log’ of the times in South Korea: Mapping the movements of coronavirus carriers.** Disponível em: https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html. Acesso em 14 jan. 2021.

UNIÃO EUROPEIA. Considerando 43 do GDPR, de 25 de maio de 2018. Regulação Geral Sobre a Proteção de Dados. **General Data Protection Regulation**. Disponível em: <https://www.privacy-regulation.eu/pt/r43.htm>. Acesso em: 22 abr. 2021.

VAIDHYANATHAN, Siva. **A Googlelização de Tudo:** (e por que devemos nos preocupar, a ameaça do controle total da informação por meio da maior e mais bem-sucedida empresa do mundo virtual. São Paulo: Cultix, 2011.

ZANATTA, Rafael A. F. **Internet das coisas:** privacidade e segurança na perspectiva dos consumidores [contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017. Brasília: Instituto Brasileiro de Defesa do Consumidor, 2017.