Autores

Adriana Cardoso de Moraes Cansian
Aluísio de Freitas Miele
Caio Henrique de Moraes Cintra
Cristiano Colombo
Daniela Monte Serrat Cabella
Débora Batista Araújo
Dionéia Motta Monte-Serrat
Eduardo Goulart Pimenta
Flávia Parra Cano
Gabriel Franco Jallais
Gabriel Ribeiro de Lima
Giovanni Carlo Batista Ferrari
José Luiz de Moura Faleiros Júnior
Júlia Lio Rocha Camargo
Lucas Enriquez Rocha
Maique Barbosa de Souza
Marcela Mattiuzzo
Marcelo de Oliveira Milagres
Natália Cristina Chaves
Pedro Henrique Magalhães Lima
Pietra Daneluzzi Quinelato
Renata Capriolli Zocatelli Queiroz
Tales Calaza
Victor Takashi Hayashi
Vívian Costa Marques
Wilson Engelmann

Leonardo **PARENTONI**
Michele **NOGUEIRA**
Coordenadores

Anne Isabelle Rodrigues de **Carvalho**
José Luiz de Moura **Faleiros Júnior**
Júlia Lio Rocha de **Camargo**
Tales **Calaza**
Organização

DIREITO, TECNOLOGIA E INOVAÇÃO

vol. 5: Internet das Coisas (IoT)

DTIBR

"Antes de abordar a Internet das Coisas (*Internet of Things* ou simplesmente IoT) é preciso compreender o que se considera tecnicamente como coisa. Essa discussão vem sendo desenvolvida, primordialmente, no ramo jurídico dos Direitos Reais (lembrando que *res*, do latim, significa coisa). Pouca ou nenhuma discussão há quanto ao fato de que circuitos eletrônicos, veículos e eletrodomésticos são coisas. Mas a complexa infraestrutura organizada para possibilitar a conexão entre eles, em tempo real, viabilizando a exploração econômica de determinados serviços, também se enquadra no conceito técnico-jurídico de coisa? Esta segunda resposta não é tão trivial quanto a primeira...

(...) Importante também destacar que este livro é o 5º volume da série intitulada "Direito, Tecnologia e Inovação", patrocinada há vários anos pelo Centro de Pesquisa em Direito, Tecnologia e Inovação – DTIBR. Assim como os volumes anteriores, este também é fruto da disciplina lecionada na Pós-Graduação da Faculdade de Direito da UFMG, nos cursos de mestrado e doutorado, sob a coordenação do Prof. Leonardo Parentoni . Sendo que neste caso a Professora Michele Nogueira, do Departamento de Ciências da Computação da UFMG e reconhecida especialista em IoT, participou como Co-coordenadora, enfocando a parte computacional do tema.

O presente livro compreende 17 textos, alguns deles fruto dos melhores trabalhos apresentados pelos alunos da disciplina, além da contribuição de autores convidados. Quanto à estrutura, o livro se divide em cinco partes. A Parte I é introdutória, contendo textos que buscam explicar ao leitor, didaticamente, no que consiste uma infraestrutura de IoT, quais são os seus principais componentes e como ela funciona. Além de analisar a legislação da União Europeia e algumas propostas brasileiras. A Parte II concentra-se na atuação profissional em IoT e na correspondente responsabilidade civil dos agentes, revisitando institutos clássicos, como a responsabilidade civil "pelo fato da coisa", de modo a adaptar tais institutos às peculiaridades da nova tecnologia. Na sequência, a Parte III enfoca um dos temas mais associados à IoT pela literatura especializada: proteção de dados pessoais. Afinal, essas "coisas" conectadas em enormes infraestruturas são capazes de coletar e processar automaticamente uma multiplicidade de dados pessoais, muitas vezes sem as cautelas necessárias e sem que os respectivos titulares dos dados sequer tenham ciência disso. A Parte IV, por sua vez, trata de outro tema indissociavelmente ligado à IoT: segurança da informação e cibersegurança, explicando o que significam tecnicamente esses conceitos e como a IoT acarreta novos desafios nessa área, aspecto ilustrado a partir da análise de regulações estrangeiras de referência, como a "Lei de Ciber Resiliência" da União Europeia (*Cyber Resilience Act*) e a "Lei de Segurança Cibernética" da China (*Cybersecurity Law of the People's Republic of China*), além do contexto brasileiro envolvendo a expansão da tecnologia 5G, por ser uma das tecnologias estruturantes dos sistemas de IoT. Finalmente, a Parte V encerra o livro trazendo textos sobre algumas situações específicas que podem se relacionar à Internet das Coisas e acarretar importantes consequências jurídicas: herança digital, metaverso e hologramas".

Trecho do Prefácio do Coordenador LEONARDO PARENTONI

DTIBR
CENTRO DE PESQUISA EM DIREITO, TECNOLOGIA E INOVAÇÃO
WWW.DTIBR.COM

9 786599 837012

DIREITO, TECNOLOGIA E INOVAÇÃO

vol. 5: Internet das Coisas (IoT)

Autores

Adriana Cardoso de Moraes Cansian
Aluísio de Freitas Miele
Caio Henrique de Moraes Cintra
Cristiano Colombo
Daniela Monte Serrat Cabella
Débora Batista Araújo
Dionéia Motta Monte-Serrat
Eduardo Goulart Pimenta
Flávia Parra Cano
Gabriel Franco Jallais
Gabriel Ribeiro de Lima
Giovanni Carlo Batista Ferrari
José Luiz de Moura Faleiros Júnior
Júlia Lio Rocha Camargo
Lucas Enriquez Rocha
Maique Barbosa de Souza
Marcela Mattiuzzo
Marcelo de Oliveira Milagres
Natália Cristina Chaves
Pedro Henrique Magalhães Lima
Pietra Daneluzzi Quinelato
Renata Capriolli Zocatelli Queiroz
Tales Calaza
Victor Takashi Hayashi
Vívian Costa Marques
Wilson Engelmann

Leonardo **PARENTONI**
Michele **NOGUEIRA**
Coordenadores

Anne Isabelle Rodrigues de **Carvalho**
José Luiz de Moura **Faleiros Júnior**
Júlia Lio Rocha de **Camargo**
Tales **Calaza**
Organização

DIREITO, TECNOLOGIA E INOVAÇÃO

vol. 5: Internet das Coisas (IoT)

Belo Horizonte - MG
2023

DIREITO, TECNOLOGIA E INOVAÇÃO – V. 5:
INTERNET DAS COISAS (IOT)

Coordenação Leonardo Parentoni
Michele Nogueira

Organização e revisão Anne Isabelle Rodrigues de Carvalho
José Luiz de Moura Faleiros Júnior
Júlia Lio Rocha Camargo
Tales Calaza

Capa José Luiz de Moura Faleiros Júnior

Diagramação José Luiz de Moura Faleiros Júnior

Centro de Pesquisa em Direito, Tecnologia e Inovação – Centro DTIBR
CNPJ/MF nº 32.727.924/0001-80
Rua dos Timbiras, 1925, Sala 903, Lourdes, Belo Horizonte/MG, Brasil
CEP 30140-069
www.dtibr.com

Fechamento da edição: 07/2023.

Dados Internacionais de Catalogação na Publicação (CIP)

D598
2023

Direito, tecnologia e inovação – v. V: Internet das Coisas (IoT) / Leonardo Parentoni, Michele Nogueira [coordenadores]; Anne Isabelle Rodrigues de Carvalho, José Luiz de Moura Faleiros Júnior, Júlia Lio Rocha Camargo, Tales Calaza [organizadores]. Belo Horizonte: Centro DTIBR, 2023.
412 p.

Inclui bibliografia.
Obra coletiva. Vários autores.
DOI: https://doi.org/10.59224/dti5
ISBN: 978-65-998370-1-2

1. Direito. 2. Direito digital. 3. Direito, tecnologia e inovação. I. Parentoni, Leonardo. II. Nogueira, Michele. III. Carvalho, Anne Isabelle Rodrigues de. IV. Faleiros Júnior, José Luiz de Moura. V. Camargo, Júlia Lio Rocha. VI. Calaza, Tales.

CDU: 340/CDD: 342.2

Catalogação na fonte

"A natureza da Internet das Coisas requer um arcabouço jurídico heterogêneo e diferenciado que leve em consideração adequadamente a globalidade, verticalidade, ubiquidade e tecnicidade da mesma". (tradução livre)

"*The nature of the Internet of Things asks for a heterogeneous and differentiated legal framework that adequately takes into account the globality, verticality, ubiquity and technicity of it*".

(WEBER, Rolf W. Internet of Things: new security and privacy challenges. *Computer Law & Security Review*, v. 26, 2010. p. 30)

Prefácio

Antes de abordar a Internet das Coisas (*Internet of Things* ou simplesmente IoT) é preciso compreender o que se considera tecnicamente como *coisa*. Essa discussão vem sendo desenvolvida, primordialmente, no ramo jurídico dos Direitos Reais (lembrando que *res*, do latim, significa coisa). Pouca ou nenhuma discussão há quanto ao fato de que circuitos eletrônicos, veículos e eletrodomésticos são coisas. Mas a complexa infraestrutura organizada para possibilitar a conexão entre eles, em tempo real, viabilizando a exploração econômica de determinados serviços, também se enquadra no conceito técnico-jurídico de coisa? Esta segunda resposta não é tão trivial quanto a primeira...

Discutindo o referido conceito, em 1938, o jurista italiano Francesco Carnelutti[1] destacou o entendimento dominante na época de que o termo "coisa" compreenderia exclusivamente os bens *corpóreos* (aqueles que "têm corpo", substância, que são formados por átomos e podem ser tocados). Afinal, foi com base neles que se construiu a teoria dos direitos reais. Porém, Carnelutti já alertava para o fato de que também os *incorpóreos*, dentro de certos limites, poderiam ser objeto de direitos reais.

Nas décadas seguintes, principalmente a partir do século XXI, o desenvolvimento tecnológico e a digitalização das informações[2] deixaram ainda mais clara a importância social e econômica dos bens incorpóreos. Consequentemente, mais vozes se

1. CARNELUTTI, Francesco. *Usucapione della proprietà industriale*. Milano: Giuffrè, 1938.
2. MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data*. 2. ed. Boston/New York: Eamon Dolan/Houghton Mifflin Harcourt, 2014. p. 09. "Though the ideas of the 'information revolution' and 'digital age' have been around since the 1960s, they have only just become a reality by some measures. As recently as the year 2000, only a quarter of the stored information in the world was digital. The other three-quarters were on paper, film, vinyl LP records, magnetic cassette tapes, and the like.

   The mass of digital information then was not much (…). But because digital data expands so quickly (…) the situation quickly inverted itself. Analog information, in contrast, hardly grows at all. So in 2013 the amount of stored information in the world is estimated to be around 1,200 exabytes, of which less than 2 percent is non-digital."

posicionaram pelo seu enquadramento como objeto de direitos reais. Bom exemplo é o texto intitulado "Que coisa é a coisa?"[3], de Luciano de Camargo Penteado, no qual este autor dialogou com a citada obra de Carnelutti e veio a concluir pelo cabimento de usucapião de propriedade intelectual.

Ocorre que a inovação proporcionada pela interconexão dos dispositivos denominados de coisa (ou seja, a IoT) é muito mais profunda e abrangente do que isso. Ela não se restringe ao vetusto debate sobre o conceito jurídico de coisa, ou ao fato de que há modelos de negócio que congregam a utilização tanto de bens corpóreos quanto de incorpóreos. Afinal, modelos desse tipo existem há décadas, nos mais diversos setores econômicos, muitos antes da atual digitalização.

Com efeito, o principal traço inovador da IoT consiste em *superar* a concepção tradicional do pensamento jurídico segundo a qual coisas tendem a ser *estáticas*, no sentido de que dependem de uma ação humana direta para que produzam efeitos[4]. Na sistemática jurídica tradicional, por exemplo, é o condutor quem liga e dirige o automóvel. É o proprietário quem abastece periodicamente a geladeira. Por outro lado, a IoT possibilita que um conjunto de coisas seja organizado para *interagir em tempo real e de maneira automatizada*, analisando o ambiente ao seu redor e respondendo a ele, dentro de determinados parâmetros, *sem necessidade de intervenção humana direta*. Inclusive, dando origem a novas relações jurídicas[5]. Neste contexto, o

3. PENTEADO, Luciano de Camargo. Que coisa é a coisa? Reflexões em torno a um pequeno ensaio de Carnelutti. *Revista de Direito Privado*. São Paulo: Revista dos Tribunais, n.º 39, p. 249-258, jul./set. 2009.
Vide, também: BARBOSA, Pedro Marcos Nunes. *Direito Civil da Propriedade Intelectual*. 3. ed. Rio de Janeiro: Lumen Juris, 2016.

4. MILAGRES, Marcelo de Oliveira. *Manual de Direito das Coisas*. Belo Horizonte: D'Plácido, 2020. p. 53. "Dois mundos coexistem. Novos e antigos direitos se imbricam. Há o mercado eletrônico, desmaterializado e sem fronteiras; mas subsiste o mercado das coisas, delimitado geograficamente. A busca da sistematização não pode ignorar uma realidade complexa e mutável."

5. O que, obviamente, *não* significa que coisas sejam sujeitos de direito. Elas continuam sendo objeto de relações jurídicas. A diferença fundamental, no contexto de IoT, é que a intermediação humana, em regra, somente se faz necessária no estágio inicial de configuração do sistema. Durante o regular funcionamento de um sistema de IoT, os sujeitos envolvidos passam a responder por "decisões" que não são tomadas diretamente por eles, mas pelo próprio sistema, em tempo real,

automóvel pode (ou possivelmente poderá, num futuro próximo) ligar-se automaticamente e ir ao posto de gasolina encher o tanque, sem a presença de qualquer ser humano, sempre que o nível de combustível estiver abaixo do parâmetro pré-definido. Da mesma forma, a geladeira pode ser programada para efetuar automaticamente a compra de certos itens, online, quando houver sido consumida determinada quantidade deles. E cada item pode ser adquirido de um fornecedor diferente. É possível, ademais, que a geladeira seja programada para pesquisar o menor preço do item entre vários fornecedores, de modo a reduzir o custo de aquisição. Tais exemplos são propositadamente simplórios e, nem de longe, refletem a complexidade das atuais aplicações da IoT. Mas eles servem ao propósito de ilustrar, didaticamente, o *novo papel desempenhado pelas coisas através dos sistemas de IoT*. Algo inimaginável em 1938, quando Carnelutti discutiu a sua natureza jurídica.

Esse novo papel que as coisas assumem no contexto de IoT acarreta *possibilidades*, *desafios* e *riscos* a serem considerados[6]. Este livro abordou esses pontos, demonstrando como a Internet das Coisas tem funcionado na prática, no Brasil e no exterior. *Com enfoque em conciliar os aspectos computacionais e jurídicos do tema*.

Importante também destacar que este livro é o 5º volume da série intitulada "Direito, Tecnologia e Inovação", patrocinada há vários anos pelo Centro de Pesquisa em Direito, Tecnologia e Inovação – DTIBR[7]. Assim como os volumes anteriores,

---

ao processar inúmeros dados e variáveis.

6. RAYES, Ammar; SALAM, Samer. *Internet of Things – From Hype to Reality*: The Road to Digitization. New York: Springer, 2017. p. 156. "Very soon, the data generated by the IoT will make up the majority of all information available on the Internet and will change the face of Big Data. It will not be possible to store all this data and analyze it later. The real-time nature of these new sources of data requires that their output be evaluated in motion and in a meaningful way."

7. Todos os volumes estão disponíveis para *download*, gratuitamente, no site do Centro DTIBR (www.dtibr.com), na aba "publicações".

   O primeiro livro da série, lançado em 2018, teve cerca de mil páginas e participação de 65 coautores, provenientes de mais de 20 universidades e centros de pesquisa, do Brasil e do exterior. O foco foi trazer ao leitor uma visão panorâmica sobre os mais variados temas da área de Direito & Tecnologia, sem focar especificamente em algum deles. O livro pode ser adquirido aqui: <https://www.editoradplacido.com.br/direito-tecnologia-e-inovacao-vol1>. Acesso em: 28 dez. 2020.

   O volume II, integralmente escrito em inglês e publicado em 2021, também teve a participação de

este também é fruto da disciplina lecionada na Pós-Graduação da Faculdade de Direito da UFMG, nos cursos de mestrado e doutorado, sob a coordenação do Prof. Leonardo Parentoni[8]. Sendo que neste caso a Professora Michele Nogueira, do Departamento de Ciências da Computação da UFMG e reconhecida especialista em IoT, participou como Co-coordenadora, enfocando a parte computacional do tema.

O presente livro compreende 17 textos, alguns deles fruto dos melhores trabalhos apresentados pelos alunos da disciplina, além da contribuição de autores convidados. Quanto à estrutura, o livro se divide em cinco partes. A Parte I é introdutória, contendo textos que buscam explicar ao leitor, didaticamente, no que consiste uma infraestrutura de IoT, quais são os seus principais componentes e como ela funciona. Além de analisar a legislação da União Europeia e algumas propostas brasileiras. A Parte II concentra-se na atuação profissional em IoT e na correspondente responsabilidade civil dos agentes, revisitando institutos clássicos, como a responsabilidade civil "pelo fato da coisa", de modo a adaptar tais institutos às peculiaridades da nova tecnologia. Na sequência, a Parte III enfoca um dos temas mais associados à IoT pela literatura especializada: proteção de dados pessoais. Afinal, essas "coisas" conectadas em enormes infraestruturas são capazes de coletar e processar automaticamente uma multiplicidade de dados pessoais, muitas vezes sem as cautelas necessárias e sem que os respectivos titulares dos dados sequer tenham ciência disso. A Parte IV, por sua vez, trata de outro tema indissociavelmente ligado à IoT: segurança da informação e cibersegurança, explicando o que significam tecnicamente esses conceitos e como a IoT acarreta novos desafios nessa área, aspecto ilustrado a partir da análise de regulações estrangeiras de referência, como a "Lei de Ciber Resiliência" da União Europeia (*Cyber Resilience Act*) e a "Lei de Segurança Cibernética" da China (*Cybersecurity Law of the People's Republic of China*), além do contexto brasileiro envolvendo a

---

autores estrangeiros. Seu foco foi a análise jurídica das tecnologias de inteligência artificial.

O volume III, também lançado em 2021, dedicou-se ao estudo dos aspectos jurídicos da tecnologia *blockchain*.

O volume IV, lançado em 2022, fez uma *análise de decisões judiciais e extrajudiciais*, nacionais e estrangeiras, envolvendo Direito & Tecnologia.

8. Na área de estudos denominada "Direito, Tecnologia e Inovação". Maiores informações em: <https://pos.direito.ufmg.br/programa/projetos-de-pesquisa/?linha=1>. Acesso em: 05 jul. 2022.

expansão da tecnologia 5G, por ser uma das tecnologias estruturantes dos sistemas de IoT. Finalmente, a Parte V encerra o livro trazendo textos sobre algumas situações específicas que podem se relacionar à Internet das Coisas e acarretar importantes consequências jurídicas: herança digital, metaverso e hologramas.

Concluo este breve prefácio destacando que um dos principais desafios (senão o ponto principal) em matéria de IoT, assim como em várias outras tecnologias voltadas à automação (inteligência artificial, *blockchain*, *digital twins*, entre outros) consiste em incorporar as novas formas de automação à vida humana para delas extrair o máximo possível de benefícios e, ao mesmo tempo, instituir mecanismos (computacionais, jurídicos e econômicos) capazes de eliminar ou ao menos mitigar seus efeitos adversos. Sempre tendo em mente que o foco é a pessoa. *Coisas são instrumentos*.

Belo Horizonte/MG, outubro de 2023.

LEONARDO PARENTONI

Doutor em Direito Comercial pela USP. Mestre em Direito Empresarial pela UFMG. Professor Adjunto da Faculdade de Direito da UFMG e Titular do IBMEC/MG. Ex-Conselheiro da composição original do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), nomeado pela Presidência da República. Fundador e Coordenador da área de concentração em Direito, Tecnologia e Inovação na Pós-Graduação da Faculdade de Direito da UFMG. Pesquisador Visitante na Universidade do Texas em Austin/USA e na Autoridade Nacional de Proteção de Dados do Uruguai. Parceiro tecnológico estratégico na Universidade de Tecnologia de Sydney. Mentor de Equipe no Programa Law Without Walls – LWOW/USA. Procurador Federal/AGU.

Apoio institucional

Centro de Pesquisa em Direito, Tecnologia e Inovação – Centro DTIBR

O Centro de Pesquisa em Direito, Tecnologia e Inovação - Centro DTIBR é uma associação sem fins econômicos, composta por equipe multidisciplinar, com o propósito de conectar o meio acadêmico e a iniciativa privada, para o treinamento de pessoas e a disseminação de conteúdo, bem como o desenvolvimento de produtos e serviços inovadores na área de Direito e Tecnologia. Sempre mantendo o compromisso com a profundidade científica das atividades e o respeito aos mais elevados padrões éticos. Conheça mais a respeito no site (https://www.dtibr.com/) ou no Facebook (https://www.facebook.com/CentroDTIBR/), Instagram (https://www.instagram.com/centrodtibr/) e LinkedIn (https://pt.linkedin.com/company/centrodtibr).

Breves currículos dos coordenadores e dos autores

Coordenadores

Leonardo Parentoni

Tem 20 anos de experiência nos setores público e privado. É Doutor em Direito pela USP. Mestre em Direito Empresarial pela UFMG. Procurador Federal/AGU. Professor da UFMG e do IBMEC/MG. Fundador e Conselheiro Científico do Centro de Pesquisa em Direito, Tecnologia e Inovação – DTIBR (www.dtibr.com). Fundador e Coordenador da área de concentração em Direito, Tecnologia e Inovação na Pós-Graduação da Faculdade de Direito da UFMG. Membro do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Ex-membro de Comissões do Conselho Nacional de Justiça, do Conselho da Justiça Federal, da Procuradoria-Geral Federal e da OAB/MG. Pesquisador Visitante na Universidade do Texas em Austin/USA e na Agência de Proteção de Dados do Uruguai. Parceiro tecnológico estratégico na Universidade de Tecnologia de Sydney. Mentor de Equipe no Programa Law

Without Walls – LWOW/USA. Principais áreas de atuação: 1) Direito, Tecnologia e Inovação; 2) Direito Societário; 3) Análise Empírica do Direito (*Empirical Legal Studies - ELS*). Número de Identificação como Pesquisador Internacional (*Researcher ID*): N-5627-2015. Publicações disponíveis gratuitamente em:

https://www.researchgate.net/profile/Leonardo-Parentoni

Michele Nogueira

Cientista da computação atuando nas áreas de redes de computadores, segurança de redes e privacidade dos dados. Membro titular do Conselho Nacional de Proteção dos Dados Pessoais e da Privacidade (CNPD) da Autoridade Nacional de Proteção dos Dados Pessoais (ANPD). Possui doutorado em Ciência da Computação pela Sorbonne Université - UPMC/LIP6, Paris, França (2009) e realizou Pós-doutorado na Universidade Carnegie Mellon (CMU), Pittsburgh, EUA, com bolsa de Estágio Pós-Doutoral no Exterior CAPES, Programas Estratégicos - DRI. É professora associada do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG) e é membro permanente do programa de Pós-graduação em Ciência da Computação. Foi professora do Departamento de Informática da Universidade Federal do Paraná (UFPR)(2010-2020). É membro sênior da Association for Computing Machinery (ACM) e do Institute of Electrical and Electronics Engineers (IEEE) em reconhecimento à sua liderança e contribuições técnicas e profissionais. Dedica-se a pesquisas voltadas à segurança e à resiliência de redes e comunicação sem fio com aplicações em vários setores da sociedade, tais como saúde e transportes. Suas pesquisas têm resultado na proposição de modelos matemáticos, protocolos e arquiteturas de sistemas. Foi bolsista CAPES do Programa de Doutorado Pleno no Exterior e foi pesquisadora visitante do laboratório BWN (Broadband Wireless Networks) no Instituto de Tecnologia da Geórgia (GeorgiaTech), Atlanta, EUA. Possui atuação ativa em sua área de pesquisa. Coordena diversos projetos de pesquisa e inovação, dentre eles o projeto temático MCTI/CGI.br/FAPESP MENTORED, cujo objetivo é realizar desde a modelagem até a experimentação de soluções contra ataques DDoS no contexto da Internet das Coisas (IoT). É autora do primeiro livro no Brasil que trata do uso de comunicação sem fio na área da saúde publicado em 2010 sob o título "Saúde Móvel: Conceitos, Iniciativas e Aplicações", e um dos inventores da solução de autenticação/segurança para IoT (United States Patent and Trademark Office No. 62287832). A pesquisadora foi agraciada, em conjunto com seus colaboradores e orientados, por dez vezes com prêmios de melhor artigo e menção honrosa em eventos nacionais e internacionais. Foi também coorientadora da melhor dissertação de mestrado

na área de segurança em sistemas computacionais, biênio 2010-2012. Foi membro do comitê consultivo da Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação. Foi editora técnica associada do periódico "IEEE Communications Magazine" (2012-2020) e dos periódicos "Computer Communications", "Journal of Network and Systems Management". É editora associada dos periódicos "IEEE Communications Surveys & Tutorials" e "IEEE Network Magazine". Coordenou o Comitê Técnico da Internet do IEEE ComSoc (2019-2021) e a Comissão Especial de Segurança da Informação e de Sistemas Computacionais (CESeg) da SBC (2020-2022). É representante da IEEE ComSoc no IEEE Systems Council e member-at-large do IEEE Strategic Planning Standing Committee.

Equipe de apoio

Anne Isabelle Rodrigues de Carvalho

Graduanda em Ciência da Computação na UFMG. E-mail: anneisabelle@ufmg.br

José Luiz de Moura Faleiros Júnior

Doutorando em Direito pela Universidade Federal de Minas Gerais e pela Universidade de São Paulo. Especialista em Direito Digital, Direito Civil e Direito Empresarial. Advogado. E-mail: jfaleiros@ufmg.br

Júlia Lio Rocha Camargo

Mestranda em Direito, Tecnologia e Inovação pela UFMG. Pós-graduada em Compliance, Ética e Governança Corporativa pela PUC Minas. Bacharel em Direito. Professora Auxiliar de Pós-Graduação na PUC Minas. Advogada Corporativa. E-mail: julialrcamargo@gmail.com

Tales Calaza

Mestrando em Direito pela Universidade Federal de Minas Gerais (UFMG). Pós-graduado em Processo Civil e em Direito do Consumidor na Era Digital pela UniDomBosco. Pós-graduado em Direito Digital pela Uniftec em parceria com o Instituto New Law. Extensão em Direito Contratual pela Harvard University. Advogado. E-mail: tales.calaza@gmail.com

Autores

Adriana Cardoso de Moraes Cansian

Advogada Especialista e Direito Digital. Doutora em Direito Comercial.

Aluísio de Freitas Miele

Mestre em Direito e Desenvolvimento pela Universidade de São Paulo. Sócio no Miele e Manini Sociedade de Advogados.

Caio Henrique de Moraes Cintra

Advogado Especialista em Direito Digital e Proteção de Dados pela Escola Brasileira de Direito – EBRADI. Certificado EXIN Privacy and Data Protection Essentials based on LGPD. Coautor do Livro LGPD x Campanha Eleitoral: Perspectivas e Desafios.

Cristiano Colombo

Pós-Doutor em Direito, Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Doutor e Mestre em Direito, Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul (UFRGS). Professor Permanente do Mestrado Profissional em Direito da Empresa e dos Negócios da UNISINOS; Pesquisador FAPERGS em Projeto: "Inteligência Artificial e Proteção de Dados Pessoais: Diálogos entre princípios da Centralidade do ser Humano e Eticidade rumo à concretização no ordenamento jurídico brasileiro." Membro da Red Iberoamericana de Universidades e Institutos con investigación en Derecho e Informática (RED CIIDDI). E-mail: cristianocolombo@unisinos.br

Daniela Monte Serrat Cabella

Advogada Especialista em Proteção de Dados e Privacidade. Co-Fundadora da Complete Privacy.

Débora Batista Araújo

Fellow of Information Privacy – IAPP; Certificações CIPP/E, CIPM – IAPP; Data Protection Officer certificada pela Universidade de Maastricht; Especialista em Direito da Economia e da Empresa – FGV/SP; Especialista em Direito Societário – Insper; Especialista em Direito Contratual – PUC/SP; Cursando LL.M em Privacidade, Cybersegurança e Gerenciamento

de Dados, pela Universidade de Maastricht (conclusão 2023). Advogada.

Dioneia Motta Monte-Serrat

Pesquisadora Colaboradora no Depto. de Computação e Matemática, FFCLRP-USP. Profa. Assistente Doutora na Universidade de Ribeirão Preto, Unaerp. Advogada.

Eduardo Goulart Pimenta

Doutor e Mestre em Direito Empresarial – UFMG. Professor Associado de Direito Empresarial na UFMG. Professor Adjunto da Faculdade de Direito da PUC/MG. Procurador do Estado de Minas Gerais. Consultor e árbitro

Flávia Parra Cano

Graduanda em Direito na Universidade de São Paulo com ênfase em teoria do direito, direito digital, proteção de dados e direitos humanos. Foi bolsista no PET (Programa de Educação Tutorial) - Sociologia Jurídica sob a tutoria do Professor Associado Rafael Mafei Rabelo Queiroz, no qual desenvolveu Iniciação Científica em direito urbanístico, apresentada no IX EPED. Realizou intercâmbio acadêmico na Universiteit Leiden com Bolsa Mérito Acadêmico da USP e faz parte do Partenariat International Triangulaire dEnseignement Supérieur (PITES) em parceria com a Université Jean Moulin Lyon 3. É pesquisadora voluntária no projeto Agenda de Emergência do Centro de Análise da Liberdade e do Autoritarismo (Laut), além de ser estagiária no escritório Rennó Penteado Sampaio Advogados. Foi monitora de graduação nas disciplinas: Introdução ao Estudo do Direito I, Disciplina Jurídica do Mercado, Empresa e Direitos Humanos, Sociologia Jurídica e Fundamentos do Direito da Empresa e da Atividade Negocial.

Gabriel Franco Jallais

Graduando em Ciência da Computação pela Universidade Federal de Minas Gerais.

Gabriel Ribeiro de Lima

Mestrando em Direito, Tecnologia e Inovação pela Universidade Federal de Minas Gerais. Pós-graduado em Direito de Uso e Proteção dos Dados Pessoais pela PUC Minas. Bacharel em Direito pela Universidade UNA. Bacharel em Administração com ênfase em Comércio Exterior pela Universidade UNA. Advogado.

Giovanni Carlo Batista Ferrari

Graduado em Direito na Universidade Federal de Minas Gerais. Pós-graduado em Direito Digital e Direito do Consumidor. Advogado.

José Luiz de Moura Faleiros Júnior

Doutorando em Direito pela Universidade Federal de Minas Gerais e pela Universidade de São Paulo. Especialista em Direito Digital, Direito Civil e Direito Empresarial. Advogado. E-mail: jfaleiros@ufmg.br

Júlia Lio Rocha Camargo

Mestranda em Direito, Tecnologia e Inovação pela UFMG. Pós-graduada em Compliance, Ética e Governança Corporativa pela PUC Minas. Bacharel em Direito. Professora Auxiliar de Pós-Graduação na PUC Minas. Advogada Corporativa.

Lucas Enriquez Rocha

Graduado em Direito pela Faculdade de Direito da Universidade de São Paulo – USP/Largo de São Francisco. Participante de duas edições consecutivas do BRICS International School (2020 e 2021), programa científico internacional voltado para pesquisadores e estudantes dos países-membros do BRICS (Brasil, Rússia, Índia, China e África do Sul). Desenvolve pesquisa sobre os impactos da tecnologia 5G quanto ao direito à privacidade no contexto brasileiro. Contato: lucas.ler@alumni.usp.br

Maique Barbosa de Souza

Mestre em Direito da Empresa e Negócios pela Universidade do Vale do Rio dos Sinos (UNISINOS). Email: maique.b.souza@gmail.com

Marcela Mattiuzzo

Doutoranda em Direito Comercial na Universidade de São Paulo, pela qual também é Mestra em Direito Constitucional. Foi membro do grupo Constituição, Política e Instituições na mesma universidade, é hoje coordenadora do Núcleo de Direito Concorrencial e Economia Digital (Nuced) da Faculdade de Direito da USP e sócia de VMCA Advogados. Foi

pesquisadora visitante na Yale Law School (2016-2017), Chefe de Gabinete e Assessora da Presidência do Conselho Administrativo de Defesa Econômica (2015-2016).

Marcelo de Oliveira Milagres

Professor Associado na Faculdade de Direito da UFMG.

Natália Cristina Chaves

Doutora em Direito pela Universidade Federal de Minas Gerais. Professora de Direito Empresarial da Faculdade de Direito da UFMG. Sócia fundadora da Passos e Chaves Sociedade de Advogados.

Pedro Henrique Magalhães Lima

Mestrando em Direito pela Universidade Federal de Minas Gerais (UFMG). Pós-graduado em Direito Constitucional pela Universidade Anhanguera. Juiz Federal.

Pietra Daneluzzi Quinelato

Doutoranda em Direito Civil na Universidade de São Paulo. Coordenadora de Direito Digital do Mansur Murad Advogados.

Renata Capriolli Zocatelli Queiroz

Advogada. Pós-Doutoranda e Doutora pela Faculdade de Direito da Universidade de São Paulo – USP. Mestre e especialista pela Universidade Estadual de Londrina - UEL. Professora Convidada do Programa de Mestrado Profissional em Direito, Sociedade e Tecnologia da Escola de Direito das Faculdades Londrina. Professora da Pós-Graduação em Direito Empresarial aplicado à era Digital da Universidade Estadual de Londrina. Professora da Faculdades Londrina.

Tales Calaza

Mestrando em Direito pela Universidade Federal de Minas Gerais (UFMG). Pós-graduado em Processo Civil e em Direito do Consumidor na Era Digital pela UniDomBosco. Pós-graduado em Direito Digital pela Uniftec em parceria com o Instituto New Law. Extensão em Direito Contratual pela Harvard University. Advogado.

Victor Takashi Hayashi

Mestre em Engenharia da Computação pela Escola Politécnica da USP.

Vívian Costa Marques

Mestranda em Direito pela Universidade Federal de Minas Gerais (UFMG), área P-08 (negócios no sistema financeiro nacional – tutela penal e administrativa). Pós-graduada em Direito das sucessões pela EBRADI. Especialista em Investimentos pela ANBIMA (CEA). Advogada.

Wilson Engelmann

Pós-Doutor em Direito Público-Direitos Humanos, Universidade de Santiago de Compostela, Espanha; Doutor e Mestre em Direito Público, Programa de Pós-Graduação em Direito da Unisinos; Professor e Pesquisador do Programa de Pós-Graduação em Direito - Mestrado e Doutorado - da UNISINOS; Bolsista de Produtividade em Pesquisa do CNPq; Pesquisador FAPERGS em Projeto: "Inteligência Artificial e Proteção de Dados Pessoais: Diálogos entre princípios da Centralidade do ser Humano e Eticidade rumo à concretização no ordenamento jurídico brasileiro.". Membro da Red Iberoamericana de Universidades e Institutos con investigación en Derecho e Informática (RED CIIDDI). E-mail: wengelmann@unisinos.br

Sumário

II

RESPONSABILIDADE CIVIL, ATUAÇÃO PROFISSIONAL
E ILÍCITOS CIVIS

IV
INTERNET DAS COISAS E
CIBERSEGURANÇA

I
ASPECTOS INTRODUTÓRIOS

INTERNET DAS COISAS (IoT) NO BRASIL E NA UNIÃO EUROPEIA:
UM ESTUDO COMPARATIVO DO ESTADO DA ARTE DA LEGISLAÇÃO SOBRE O TEMA

Tales Calaza

Mestrando em Direito pela Universidade Federal de Minas Gerais (UFMG). Pós-graduado em Processo Civil e em Direito do Consumidor na Era Digital pela UniDomBosco. Pós-graduado em Direito Digital pela Uniftec em parceria com o Instituto New Law. Extensão em Direito Contratual pela Harvard University. Advogado.

DOI: https://doi.org/10.59224/dti5.ch1

Resumo: O tema "Internet das Coisas" é recente e apresenta grandes desafios regulatórios que podem impactar nas mais diversas áreas do direito. O presente capítulo tem por objetivo analisar o estado da arte da legislação sobre a IoT no Brasil em comparação com a União Europeia (bloco econômico que se revela na vanguarda regulatória do tema), de modo a contextualizar os principais desafios e problemáticas comuns aos territórios indicados. Finalmente, objetiva analisar se há soluções internacionais que podem ser "importadas" para o cenário nacional, no que tange a regulação da tecnologia indicada.

Palavras-chave: Internet das Coisas; União Europeia; legislação.

***Abstract*:** *The theme "Internet of Things" is recent and presents significant regulatory challenges that can impact various areas of law. This chapter aims to analyze the state of the art of legislation on IoT in Brazil in comparison with the European Union (economic block that is at the forefront of regulatory issues on the topic), in order to contextualize the main challenges and common issues in the indicated territories. Finally, it aims to analyze whether there are international solutions that can be "imported" into the national scenario regarding the regulation of the indicated technology.*

Keywords: *Internet of Things; European Union; legislation.*

SUMÁRIO: 1. Introdução; 2. Análise evolutiva e contemporânea da legislação da IoT no contexto nacional; 3. Análise evolutiva e contemporânea da legislação da IoT no contexto europeu; 4. Perspectivas para o futuro da regulação da IoT no Brasil; 5. Conclusão; Referências.

1. INTRODUÇÃO

Em meados da década de 1960, a internet foi originalmente desenvolvida com a finalidade de conectar computadores e transmitir mensagens com tamanhos limitados e formatos restritos. Com o avançar das tecnologias, foi possibilitado ao usuário interagir com documentos disponíveis em uma rede mundial de computadores (Web 1.0), compartilhar formatos diferentes de mídia - como voz e vídeo – ao gerar dados e conteúdos a partir de seu próprio dispositivo (Web 2.0) e, recentemente, vislumbrar dispositivos conectados entre si, coletando, armazenando e compartilhando dados, nos meios público e privado (Web 3.0)[1].

Neste cenário de objetos conectados, surge o conceito de Internet das Coisas (IoT)[2], utilizado para designar essa infraestrutura/ecossistema no qual tais dispositivos comunicam e interagem. Todavia, esta tecnologia não se limita a criação de uma nova infraestrutura, mas também impacta diretamente na criação de novos *hardwares* (dispositivos que serão conectados à IoT), *softwares* (plataformas e sistemas de IoT) e serviços (aplicações/aplicativos de IoT).

Em um primeiro contato com uma aplicação prática da IoT, o usuário pode ficar deslumbrado ao se deparar com cenários como: a) conversar com uma assistente pessoal contida em um dispositivo que está na cabeceira de sua cama e, instantaneamente, ver suas palavras se transformarem em uma lista de compras em seu celular[3]; ou mesmo b) apagar as luzes de sua residência via tablet após ter saído da cidade[4], ao

1. *Staff Working Document: Advancing the Internet of Things in Europe*. European Comission, 2016. Disponível em: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-advancing-internet-things-europe. Acesso em: 05 de julho de 2022.
2. O primeiro uso do termo "Internet das Coisas" (*internet of things*) foi atribuído à Kevin Ashton, fundador do *Auto-ID Center* no *Massachusetts Institute of Technology*. Na oportunidade, teria afirmado a necessidade de uma "Internet das Coisas de modo a criar um padrão para que os computadores capturassem as informações do mundo real e as entendessem". Informação disponível em: *Staff Working Document: Advancing the Internet of Things in Europe*. European Comission, 2016. Disponível em: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-advancing-internet-things-europe. Acesso em: 05 de julho de 2022.
3. KITAMURA, Celso. *Faça sua lista de compras com a Alexa*. Celso Kitamura, 2021. Disponível em: https://celsokitamura.com.br/faca-sua-lista-de-compras-com-a-alexa/. Acesso em: 05 de julho de 2022.
4. MATTERE, Henrique. *Casa automatizada – Como acender luz pelo celular?* Mundo da Elétrica.

deixar apressadamente a sua casa com destino ao aeroporto em um dia agitado.

Ocorre que, com todas essas comodidades, também surgem grandes desafios[5], que podem resultar em desdobramentos a partir de uma simples coleta indevida de um dado sensível[6] até acidentes e danos reais (físicos ou psicológicos) causados por dispositivos cujos potenciais ainda não foram devidamente estudados e que não oferecem a segurança que deles se espera[7]. O tema não é simples e envolve diversas áreas do conhecimento, cujo estudo transdisciplinar se revela necessário para que tal tecnologia alcance todo o seu potencial, mas garantindo a segurança de seu usuário e de terceiros. Entre os temas tangentes ao presente estudo, é possível destacar: infraestrutura das redes, cibersegurança, proteção de dados pessoais, responsabilidade civil, contratos e relações obrigacionais, geopolítica internacional, dentre outros.

Diante deste cenário, mostra-se evidente a indispensabilidade de uma trilha normativa que regule o ecossistema da IoT com um objetivo específico: para que seus potenciais riscos não superem as comodidades e os benefícios por ela oferecidos. Nesse contexto, o presente artigo pretende explorar o estado da arte da legislação sobre o tema "Internet das Coisas" no Brasil, assim como traçar estudos comparativos internacionais com a União Europeia sobre o panorama evolutivo quanto a regulação sobre o tema.

Disponível em: https://www.mundodaeletrica.com.br/casa-automatizada-como-acender-luz-pelo-celular/. Acesso em: 05 de julho de 2022.

5. *However, despite its tremendous potential and benefits, IoT is expected to create significant challenges for policymakers and enterprises across demand, business model, and technology*. Citação disponível em: *Enabling the IoT ecosystem with a policy and regulation*. Synergy Consulting. Disponível em: https://www.synergyconsulting.ae/insights/enabling-iot-ecosystem-policy-regulation/. Acesso em: 05 de julho de 2022.
6. Sobre o tema, ver o filme Smart House da Disney, datado de 1999, especificamente no que tange ao trecho a seguir: https://www.youtube.com/watch?v=RxUZb3WnTpo&ab_channel=DisneyChannel. Logo nos primeiros segundos do vídeo, se verifica a colheita de dados biométricos de uma criança, como suas digitais e até seu sangue, com a justificativa de que, com esses dados, o dispositivo (no caso, a Smart House) conheceria melhor seu usuário.
7. Sobre o tema, ver episódio da série Mr. Robot (https://www.youtube.com/watch?v=aAj8zHOEfiI&ab_channel=Alex.Under.Ros.1980) e episódio do desenho Mickey Mouse (https://www.filmaffinity.com/es/film663644.html). Em ambos, é possível verificar o potencial danoso de dispositivos conectados sem a devida regulação.

2. ANÁLISE EVOLUTIVA E CONTEMPORÂNEA DA LEGISLAÇÃO DA IOT NO CONTEXTO NACIONAL

A primeira vez que o termo "Internet das Coisas" foi citado em uma norma oficial nacional de âmbito federal foi no ano de 2016, no Decreto nº 8.776 (hoje já revogado), que instituiu o Programa Brasil Inteligente. Por conta de sua novidade e seu estado regulatório incipiente, essa primeira norma fez menção ao termo de forma tímida, de modo que somente pode ser localizado em uma oportunidade ao longo de toda a redação do documento, sendo caracterizado como "um dos objetivos do Programa Brasil Inteligente para alcançar a finalidade de buscar a universalização do acesso à internet no país". Até então, não havia nenhum aspecto regulatório específico sobre o tema.

A partir deste marco inicial em 2016, é possível localizar outras oito normas que citam o termo "Internet das Coisas" de forma expressa[8], das quais duas foram publicadas em 2018[9], três em 2019[10], duas em 2020[11] e uma em 2021[12]. Das nove normas nacionais que se referem expressamente ao tema, sete delas estão em vigor e, dentre estas, quatro citam o termo "Internet das Coisas" em mais de uma oportunidade. As

8. Os resultados da pesquisa podem ser localizados em: *"Internet das Coisas"*. Legislação Federal Brasileira. Disponível em: https://legislacao.presidencia.gov.br/#. Acesso em: 10 de julho de 2022.
9. Decreto nº 9.319/2018 (em vigor), que instituiu o Sistema Nacional para a Transformação Digital e estabeleceu a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital; e Decreto nº 9.557/2018 (em vigor), que estabeleceu requisitos obrigatórios para a comercialização de veículos no país e instituiu o Programa Rota 2030.
10. Decreto nº 9.677/2019 (revogado), que aprovou a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança do Ministério da Ciência, Tecnologia, Inovações e Comunicações; Decreto nº 9.689/2019 (em vigor), que dispôs sobre funções comissionadas técnicas e gratificações, transformou cargos em comissão e alterou decretos de estrutura regimental; e Decreto nº 9.854/2019 (em vigor), que instituiu o Plano Nacional de Internet das Coisas.
11. Decreto nº 10.222/2020 (em vigor), que aprovou a Estratégia Nacional de Segurança Cibernética; e Decreto nº 10.463/2020 (em vigor), que aprovou a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança do Ministério da Ciência, Tecnologia e Inovações.
12. Decreto nº 10.609/2021 (em vigor), que instituiu a Política Nacional de Modernização do Estado e o Fórum Nacional de Modernização do Estado.

outras três normas que estão em vigor citam o termo IoT somente uma vez no decorrer de sua redação e não se revestem de caráter regulatório quanto ao tema em estudo, restringindo-se a utilizar a expressão indicada para fins de contextualização. O mesmo ocorre com o Decreto nº 9.557/2018, que cita o termo em mais de uma oportunidade, mas trata do assunto com fins meramente descritivos, sem necessariamente conter uma carga regulatória sobre o tema. Dessa forma, na contemporaneidade, são localizadas três normas em vigor no país que tratam expressamente do tema "Internet das Coisas" com finalidade além da meramente descritiva, as quais serão analisadas a seguir[13].

A título elucidativo, é apresentada a seguinte tabela para fins didáticos, no que tange a evolução legislativa tangente ao tema:

Legislação nacional tangente ao tema "Internet das Coisas"			
Norma	**Situação**	**Contexto**	**Relevância para o tema**
Decreto nº 8.776/2016	Revogado	Institui o Programa Brasil Inteligente	Institui o desenvolvimento e a adoção de soluções nacionais de IoT como um dos objetivos do Programa Brasil Inteligente, para buscar a universalização do acesso à internet no país.
Decreto nº 9.319/2018	Em vigor	Institui o Sistema Nacional para a Transformação Digital	Institui um "mundo de dispositivos conectados" como um dos eixos de transformação digital ao reconhecer o potencial transformados das aplicações de IoT.
Decreto nº 9.557/2018	Em vigor	Institui o Programa Rota 2030, sobre mobilidade e logística	Trata de aspectos sobre a tributação de componentes e equipamentos com aplicações de IoT.
Decreto nº 9.677/2019	Revogado	Aprova a estrutura do Ministério da Ciência, Tecnologia, Inovações e Comunicações	Distribui as responsabilidades sobre a execução de políticas relacionadas a IoT, nas respectivas áreas de competência.
Decreto nº	Em vigor	Dispõe sobre	Imputa ao Departamento de Ciência,

13. Em que pese somente terem sido localizados os diplomas indicados no que tange a referências diretas e expressas à Internet das Coisas, não se negligencia a existências de diversos outros normativos que regulam esta tecnologia de forma indireta.

9.689/2019		funções comissionadas técnicas e gratificações das unidades da administração pública federal	Tecnologia e Inovação Digital a competência de executar as medidas necessárias para a execução de políticas de IoT.
Decreto nº 9.854/2019	Em vigor	Institui o Plano Nacional de Internet das Coisas	Institui o Plano Nacional de Internet das Coisas com a finalidade de implementar e desenvolver a Internet das Coisas no país.
Decreto nº 10.222/2020	Em vigor	Aprova a Estratégia Nacional de Segurança Cibernética	Trata da Internet das Coisas na fase de diagnóstico para a Estratégia Nacional de Segurança Cibernética.
Decreto nº 10.463/2020	Em vigor	Aprova a Estrutura do Ministério da Ciência, Tecnologia e Inovações	Distribui as responsabilidades sobre a execução de políticas relacionadas a IoT, nas respectivas áreas de competência.
Decreto nº 10.609/2021	Em vigor	Institui a Política Nacional de Modernização do Estado	Estabelece a Internet das Coisas como um dos tópicos a serem observados dentro do eixo temático "governo e sociedade digital" para a implementação da Política Nacional de Modernização do Estado.

Tabela 1 – Legislação nacional tangente ao tema "Internet das Coisas".
Fonte: autoria própria.

Em que pese serem localizadas poucas normas regulatórias expressas sobre o tema, há diversas iniciativas anteriores que serviram como pilares para que a regulação alcançasse seu estado atual, conforme será demonstrado no decorrer do presente estudo.

O primeiro diploma que trata do tema IoT de forma além da meramente descritiva é a Política Nacional de Segurança da Informação (Decreto nº 9.637/2018[14]). A norma é datada de 2018, mas veio a se referir expressamente sobre o termo indicado somente em fevereiro de 2020, em seu anexo que aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber) que, por si só, é um Decreto à parte (Decreto nº

14. BRASIL. *Decreto nº 9.637/2018 (Política Nacional de Segurança da Informação)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art6i. Acesso em: 10 de julho de 2022.

10.222/2020[15]).

No texto indicado, em fase de diagnóstico, é reconhecido que "haverá mais de trinta bilhões de dispositivos de Internet das Coisas (IoT, do inglês Internet of Things) conectados em 2020", que "o processo de preparação do País rumo à nova economia digital, experimentará forte impacto de variadas tecnologias, como Internet das Coisas" e que "é essencial que o Brasil participe de iniciativas de estruturação normativa futura, como as relativas à criação de padrões que guiarão a segurança em tecnologias emergentes, como as redes de comunicação 5G, a inteligência artificial e a Internet das Coisas".

Apesar de a norma indicada não conter necessariamente um conteúdo regulatório expresso diretamente vinculado à IoT, é possível verificar que traz informações além de uma mera contextualização, demonstrando que o Governo Federal, à época, já havia começado a se preocupar efetivamente com o tema, reconhecendo a sua importância e o seu impacto no mercado e na tutela da segurança da informação.

Em seguida, o segundo diploma que faz referência expressa sobre a tecnologia em questão é o Decreto nº 10.463/2020[16], publicado em agosto de 2020. Assim como a norma anterior, em que pese não adentrar especificamente no mérito regulatório, a norma traz considerações relevantes no que tange a organização do Ministério da Ciência, Tecnologia e Inovações, que preside a Câmara IoT (órgão de assessoramento destinado a acompanhar a implementação e o desenvolvimento na Internet das Coisas no país).

Na prática, o diploma indicado define a seguinte atribuição para a Secretaria de Empreendedorismo e Inovação: "propor, coordenar e acompanhar a execução do Plano Nacional de Internet das Coisas, e ações voltadas para o desenvolvimento tecnológico, empreendedorismo e a inovação relacionadas à Saúde 4.0, ao Agro 4.0, à Cidades 4.0 e à Indústria 4.0".

Na oportunidade, delega para o Departamento de Ciência, Tecnologia e Inovação

15. BRASIL. *Decreto nº 10.222/2020 (Estratégia Nacional de Segurança Cibernética)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 10 de julho de 2022.
16. BRASIL. *Decreto nº 10.463/2020*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10463.htm. Acesso em: 10 de julho de 2022.

Digital (departamento vinculado à Secretaria de Empreendedorismo e Inovação), as seguintes atribuições: a) "executar as medidas necessárias à execução das políticas de informática, tecnologias da informação e comunicação, inovação digital, Internet das Coisas, microeletrônica e tecnologias de comunicação avançadas"; e b) "propor, coordenar e acompanhar a execução do Plano Nacional de Internet das Coisas, bem como das ações voltadas para o desenvolvimento tecnológico, empreendedorismo e a inovação relacionadas à Saúde 4.0, ao Agro 4.0, à Cidades 4.0 e à Indústria 4.0".

Em análise, verifica-se que tal delegação se revela oportuna, vez que cumprirá a um departamento específico tomar a frente nos projetos de implementação, evitando assim conflitos positivos (quando mais de um órgão entende ser competente para definir diretrizes, resultando em normativos conflitantes) ou mesmo conflitos negativos (quando nenhum órgão assume efetivamente a coordenação do projeto, por entender que a iniciativa seria de responsabilidade de outro).

Por fim, é passada à análise do primeiro diploma publicado que trouxe efetivamente o tema Internet das Coisas como objeto principal: o Plano Nacional de Internet das Coisas (Decreto nº 9.854/2019[17]), que integra a "Estratégia Brasileira para a Transformação Digital – E-Digital"[18].

Em que pese a primeira norma que teve a tutela da IoT como objeto principal no contexto nacional somente ter sido publicada no ano de 2019, diversos normativos e ações anteriores se revelaram essenciais para que fosse alcançado este primeiro marco regulatório expresso sobre o tema.

Abaixo, é possível verificar uma linha do tempo elaborada pela OCDE (Organização para a Cooperação e Desenvolvimento Econômico) com o histórico do Governo Eletrônico/Governo Digital no Governo Federal Brasileiro, que serviu de pretexto para a atual Estratégia Brasileira para a Transformação Digital:

17. BRASIL. *Decreto nº 9.854/2019 (Plano Nacional de Internet das Coisas)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9854.htm. Acesso em: 10 de julho de 2022.
18. *Estratégia brasileira para a transformação digital (E-Digital)*. Ministério da Ciência, Tecnologia e Inovações. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/estrategia-digital. Acesso em: 30 de julho de 2022.

Histórico do Governo Eletrônico/Governo Digital no Governo Federal Brasileiro	
Ano	**Marco**
2000	Política de e-Governo
	Programa Sociedade da Informação
	Comitê Executivo do Governo Eletrônico (CEGE)
2001	Infraestrutura de Chaves Públicas Brasileira - ICP Brasil
	Portal do Governo Eletrônico
2002	Portal Rede Governo
2003	Infraestrutura de Rede Infovia Brasília
	Decreto 4.829: criação do Comitê Gestor da Internet no Brasil (CGI.br)
2004	Portal da Transparência
2005	Padrões de Interoperabilidade de Governo Eletrônico (e-PING)
	Portal de Compras Públicas (Comprasnet)
	Programa Nacional de Gestão Pública e Desburocratização (Gespública)
2006	Portal de Inclusão Digital
	Pesquisa de avaliação de Serviços com Indicadores de Governo Eletrônico
2007	Modelo de Acessibilidade em Governo Eletrônico (eMAG)
	Avaliador e Simulador de Acessibilidade em Sítios (ASES)
2008	Padrões Web em Governo Eletrônico (ePWG)
	Infraestrutura Nacional de Dados Espaciais (INDE)
	Estratégia Geral de Tecnologia da Informação (EGTI)
2009	Decreto 6.932: simplificação do atendimento ao cidadão
2010	Programa Nacional de Banda Larga (PNBL)

	Pesquisa TIC Governo Eletrônico do CETIC.Br
2011	Comitê Interministerial Governo Aberto (CIGA) e Plano de Ação Nacional para Governo Aberto
2012	Portal para Pessoa com Deficiência
	Lei 12.527: Acesso à Informação
	Infraestrutura Nacional de Dados Abertos (INDA)
	Portal Brasileiro de Dados Abertos
2013	Programa Cidades Digitais
	Decreto 8.135: comunicações de dados federais
2014	Lei 12.965: Marco Civil da Internet
	Decreto 8.243: Política Nacional de Participação Social (PNPS)
	Portal Participa.br
2015	Decreto 8.414: Programa Bem Mais Simples Brasil
	Decreto 8.539: Processo Eletrônico Nacional
2016	Decreto 8.638: Política de governança digital
	Estratégia de governança digital (EGD)
	Decreto 8.777: Política de dados abertos
	Decreto 8.936: Plataforma de cidadania digital
	Decreto 8.789: Compartilhamento de bases de dados
2017	Decreto 9.094: simplificação dos serviços públicos
	Decreto 9.203: Política de governança pública
	Lei 13.444: Identificação Civil Nacional
	Conselho Nacional para a Desburocratização– Brasil Eficiente
2018	Decreto 9.319: Estratégia Brasileira para a Transformação Digital (E-Digital)

Tabela 2 – Histórico do Governo Eletrônico/Governo Digital no Governo Federal

Brasileiro. Fonte: OCDE[19] (Adaptado).

O rol acima não é taxativo. Além dos itens contidos no quadro, se destacam outros normativos e iniciativas no contexto evolutivo da regulação direta da IoT e de temas tangentes[20], como a iniciativa 04QH do PPA 2016-2019[21], a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)[22], dentre outros.

Retomando à análise do Decreto em voga, que instituiu o Plano Nacional de Internet das Coisas, verifica-se logo em seu artigo 1º a sua finalidade de implementação e desenvolvimento da Internet das Coisas no País. Ainda, este artigo traz duas relevantes informações tangentes ao tema: que o Plano terá base na livre concorrência e na livre circulação de dados e que deverão ser observadas as diretrizes de segurança da informação e da proteção de dados pessoais[23]. Tal contextualização é de extrema

19. OECD. *Revisão do Governo Digital do Brasil: rumo à transformação digital do setor público*. Disponível em: https://repositorio.enap.gov.br/bitstream/1/3627/1/2b.%20Review%20OCDE%20Governo%20Digital%20%28Portugu%C3%AAs%29.pdf. Acesso em: 30 de julho de 2022.
20. LACERDA, Flávia. *Análise ex ante do plano nacional de Internet das Coisas (IoT): ambiente cidades inteligentes*. Instituto Serzedello Corrêa, 2020.
21. "Articulação de projetos de pesquisa, desenvolvimento e inovação em áreas estratégicas de tecnologias digitais com empresas e centros de pesquisa e desenvolvimento (P&D), especialmente na área de segurança cibernética, Internet das Coisas, big data e computação em nuvem". CONGRESSO NACIONAL. Projeto plurianual da União para o período de 2016 a 2019. Disponível em:https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=C93FBE24E28C7EAF229B4AD8E0AB8BBC.proposicoesWeb1?codteor=1426481&filename=Tramitacao-PLN+6/2015+CN. Acesso em: 31 de julho de 2022.
22. Não se ignora o fato de que a Lei Geral de Proteção de Dados é uma lei geral (tecnologicamente neutra), de modo que não se revela como um marco regulatório específico para a tecnologia indicada. Entretanto, é uma lei que tutela um tema tangente à Internet das Coisas, qual seja: a proteção de dados. Por este motivo, se revela como um importante marco evolutivo para a análise da tecnologia de objeto deste estudo.
23. Por "diretrizes de segurança da informação", é possível interpretar tanto normas tidas como "boas práticas", como as ISO (*International Organization for Standardization*) da família 27000, quanto normas efetivas que tratam sobre o tema, como o Decreto nº 9.637/2018 (que instituiu a Política Nacional de Segurança da Informação). Já em relação às "diretrizes de proteção de dados pessoais", é possível identificar normas expressas já publicadas sore a temática (a exemplo da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018), como normas tangentes que tratam do assunto de forma acessória (a exemplo do Código de Defesa do Consumidor, Marco Civil da

relevância, levando em consideração que a livre concorrência (princípio da ordem econômica introduzido pela Constituição Federal de 1988, em seu artigo 170, inciso IV) se traduz como uma importante diretriz para o mercado, uma vez que busca estabelecer uma concorrência justa, não limitada a determinados agentes detentores de maior poderio econômico. Já a livre circulação de dados é uma premissa trazida pelo artigo 1º do Regulamento Europeu de Proteção de Dados (GDPR), que tem como objetivo principal a compatibilização entre os direitos e liberdades individuais do titular de dados com os interesses mercadológicos.

Em seguida, o Decreto em análise apresenta os conceitos de "Internet das Coisas", "coisas", "dispositivos" e "serviço de valor adicionado", termos estes essenciais para a interpretação do diploma indicado. Tal disposição se manifesta como uma boa prática, pois auxilia o leitor a evitar interpretações divergentes e ambíguas, vez que termos como "coisas" e "dispositivos" podem transparecer os mais diversos significados, em diferentes contextos.

Na sequência, é possível identificar que os principais objetivos do Plano Nacional de IoT são: a melhora da qualidade de vida dos cidadãos, o aumento da eficiência dos serviços, a promoção da capacitação profissional e a geração de empregos, o incremento da produtividade e a fomentação da competitividade das empresas brasileiras, a promoção de parcerias entre os setores público e privado e o aumento da integração internacional do país. É verificado que tais propósitos almejados pelo Plano estão de acordo com os Objetivos de Desenvolvimento Sustentável no Brasil[24] (Agenda 2030 da ONU), principalmente no que tange ao trabalho decente e crescimento econômico, à indústria, inovação e infraestrutura, às cidades e comunidades sustentáveis, e às parcerias e meios de implementação.

O Decreto em voga também informa que o presidente da Câmara IoT (Ministro de Estado da Ciência, Tecnologia, Inovações e Comunicações) indicará quais serão

---

Internet, entre outros diplomas já tratados neste trabalho). Veja que, por não limitar de forma expressa as normas em um rol taxativo, é necessário realizar uma leitura extensiva destas normas, não podendo serem limitadas ou restritas, em respeito aos princípios do Código de Defesa do Consumidor e à Lei Geral de Proteção de Dados, vez que a leitura extensiva beneficia a parte vulnerável na relação de consumo/tratamento de dados.

24. ONU. *Os objetivos de desenvolvimento sustentável no Brasil*. Disponível em: https://brasil.un.org/pt-br/sdgs. Acesso em: 04 de agosto de 2022.

os ambientes priorizados para aplicações de soluções de IoT, desde que inclua, no mínimo, os seguintes ambientes: saúde, cidades, indústria e rural. É possível identificar o motivo pelo qual esses quatro ambientes foram escolhidos como prioridades a partir do detalhamento do estudo da "Internet das Coisas" realizado pelo Governo Federal[25]: são áreas cujas soluções de IoT terão grande impacto no adensamento da cadeia produtiva, na competitividade dos setores econômicos do Brasil e na qualidade de vida dos cidadãos. Além disso, as áreas priorizadas também guardam coerência com os objetivos previstos na Agenda ONU 2030, conforme indicado anteriormente.

Na sequência da análise do Decreto, verifica-se que os artigos 5° e 6° definem, respectivamente, os temas[26] e projetos[27] que integrarão o Plano Nacional de Internet das Coisas, enquanto o artigo 7° do diploma cria a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas (ou somente Câmara IoT), órgão responsável pelo acompanhamento e implementação do Plano Nacional de IoT no país, assim como exemplifica as suas funções, sua natureza, sua composição e regras sobre as reuniões, orçamento e outros detalhes administrativos. Quanto as reuniões a serem realizadas pelo órgão, chama-se a atenção para uma possível problemática: associações e entidades públicas e privadas somente podem participar a convite do Secretário responsável (disposição prevista no artigo 7°, § 6°, do Decreto em análise). A problemática é levantada ao passo em que, levando em consideração que o tema IoT é multidisciplinar e impacta nos mais diversos segmentos da indústria e do mercado, a eventual limitação de participação nos encontros a determinadas entidades pode acarretar a restrição da amplitude necessária para o debate, vez que a pluralidade de opiniões e expertises é

25. *Estudo de Internet das Coisas*. Ministério da Ciência, Tecnologia e Inovações. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas-estudo. Acesso em: 10 de julho de 2022.
26. Ciência, tecnologia e inovação; inserção internacional; educação e capacitação profissional; infraestrutura de conectividade e interoperabilidade; regulação, segurança e privacidade; e viabilidade econômica.
27. Plataformas de inovação em Internet das Coisas; centros de competência para tecnologias habilitadoras em Internet das Coisas; e observatório nacional para o acompanhamento da transformação digital.

extremamente relevante para a incorporação das soluções de Internet das Coisas na indústria e na sociedade.

Por fim, os demais artigos trazem disposições gerais que se aplicam no âmbito do Plano Nacional de Internet das Coisas. Dentre eles, destacam-se as seguintes disposições que garantem um impacto positivo para a economia nacional: é permitido que os membros da Câmara IoT participem da reunião por meio de videoconferência (redução de custos com deslocamento, estadia e acessórios); eventuais custas com deslocamento e estadia que se fizerem necessárias são custeadas pelos respectivos órgãos de origem (evita delegar despesas para um novo órgão); e a participação dos membros não é remunerada (obsta a criação de novas despesas).

Diante desta análise, verifica-se que, apesar de não se encontrar em um estágio avançado de regulação sobre a tecnologia indicada, já foram iniciados no país os trabalhos para levar a atenção necessária ao tema. Dessa forma, passa-se à análise comparativa internacional no que tange ao estado da arte da legislação sobre o tema, no contexto contemporâneo da União Europeia.

3. ANÁLISE EVOLUTIVA E CONTEMPORÂNEA DA LEGISLAÇÃO DA IOT NO CONTEXTO EUROPEU

Superada a análise do estágio legislativo atual no Brasil, o presente capítulo busca aprofundar na análise dos primeiros marcos regulatórios mundiais sobre a temática da Internet das Coisas. Para os fins do presente estudo, o recorte territorial escolhido para a investigação foi a União Europeia, por se tratar de um importante bloco com influência cultural, econômica e política a nível global, além de se revelar como um pioneiro na regulação de temas tangentes ao objeto desta pesquisa.

A primeira vez que o termo *Internet of Things* foi citado de forma expressa em uma norma oficial da União Europeia foi no ano de 2006[28], no *Comission staff working paper i2010*. Assim como na primeira norma sobre o tema publicada no contexto nacional, conforme poderia se esperar por conta de sua novidade, o termo foi

28. *Comission staff working paper – i2010 – First Annual Report on the European Information Society {COM(2006)215}*. EUR-Lex. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006SC0604&qid=1657396829302. Acesso em: 09 de julho de 2022.

utilizado de forma tímida, de modo que somente pode ser localizado em uma única oportunidade ao longo do documento, sendo caracterizado como "uma das próximas áreas prováveis para que se ocorra a próxima disrupção". Até então, não há nenhum aspecto regulatório específico sobre o tema.

A partir desse marco, entre a publicação deste primeiro documento (ocorrida no ano de 2006) e o ano de elaboração do presente texto (2022) é possível localizar nada menos do que 1.015 (mil e quinze) normas oficiais da União Europeia que citam o termo "Internet das Coisas"[29], dentre eles: regulamentos, diretivas, decisões, resoluções, regulações, entre outros documentos oficiais. Este capítulo não aprofundará no mérito de cada uma destas normativas, inicialmente pelo fato de não ser possível alcançar a objetividade que este trabalho almeja a partir da análise e transcrição das conclusões de todos os documentos indicados. Em segundo lugar, não é o escopo da presente pesquisa realizar uma análise pormenorizada de toda a legislação europeia tangentes ao tema, mas sim adentrar em normas recentes e específicas, que efetivamente tratam do estado atual da regulação da IoT no contexto europeu.

Dessa forma, o marco teórico contemporâneo escolhido para análise e aprofundamento com este trabalho, em contraste com o Decreto nacional mais recente sobre o tema (Plano Nacional de Internet das Coisas), foi o *Comission staff working document – Advancing the Internet of Things in Europe*[30], publicado em 2016. Este documento foi escolhido como objeto de pesquisa por se tratar de um texto completo, contendo aspectos regulatórios, técnicos e jurídicos sobre a Internet das Coisas, além de seu conteúdo se revelar extremamente atual.

A norma indicada inicia seu texto contextualizando o que se entende pela expressão "Internet das Coisas", quais seriam os seus principais benefícios e desafios, assim como traz informações sobre a força que a União Europeia possui num contexto global em relação às tecnologias digitais, no que tange a participação ativa em grupos de

29. Os resultados da pesquisa podem ser localizados em: *"Internet of things"*. EUR-Lex. Disponível em: https://eur-lex.europa.eu/search.html?lang=en&text=%22internet+of+things%22&qid=1657396829302&type=quick&scope=EURLEX. Acesso em: 09 de julho de 2022.

30. *COMMISSION STAFF WORKING DOCUMENT Advancing the Internet of Things in Europe*. EUR-Lex. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110. Acesso em: 09 de julho de 2022.

cooperação internacional em matéria de privacidade e proteção de dados[31].

Conforme informado anteriormente, o bloco econômico europeu exerce uma influência cultural e política a nível mundial. Desta forma, se revela extremamente oportuna a presença desta introdução descritiva no documento com finalidade de contextualização, vez que o bloco indicado é formado por diversos países, cada qual ainda formado por microrregiões, cujo estado da arte desta tecnologia apresenta assimetrias entre cada território vizinho. Além disso, os *softwares* e *hardwares* que integram a infraestrutura da Internet das Coisas podem ser desenvolvidos nas mais diversas localidades, cada qual com sua regulação específica. Portanto, essa contextualização permite que os desenvolvedores, fornecedores, comerciantes e consumidores internacionais possam estar alinhados em relação ao tema, partindo de uma premissa comum, minimizando eventuais assimetrias informacionais existentes entre seus respectivos territórios de origem.

Ao avançar na leitura, o documento introduz o conceito de "*a single market for the internet of things*" (tradução livre: um mercado único para a Internet das Coisas), no qual discorre sobre relevantes detalhes técnicos necessários para que a cooperação internacional possibilite uma infraestrutura próspera para o funcionamento integrado e para a regulação da IoT e dos dispositivos conectados. Não é o objetivo do presente estudo adentrar nos aspectos técnicos da infraestrutura da tecnologia indicada, entretanto, a título elucidativo, é possível classificar a sua arquitetura em três

31. De fato, além de todas as normas e regulações indicadas no contexto europeu, o bloco também participa de diversos contextos de cooperação internacional sobre o tema. Entre eles (rol não exaustivo): Conselho da Europa (CdE), Organização para a Cooperação do Desenvolvimento Econômico (OCDE), Conferência Internacional dos Comissários para a Proteção dos Dados e Privacidade (ICDPPC), Conferência de Primavera das Autoridades de Proteção de Dados europeias, Rede Global para a Proteção da Privacidade (GPEN), Grupo de Berlim – Grupo Internacional de Proteção de Dados nas Telecomunicações (IWGDPT), Associação Francófona das Autoridades de Proteção de Dados Pessoais (AFAPDP), Autoridades de Proteção de Dados da Europa Central e Oriental (CEEDPA), Fórum para a Privacidade da Região Ásia-Pacífico (APPA), Cooperação Econômica Ásia-Pacífico (APEC), *Common Thread Network* (CTN), Rede Ibero-Americana de Proteção de Dados (RIPD) e Aliança para a Internet das Coisas (AIOTI). Saiba mais em: *Cooperação internacional*. European Data Protection Board. Disponível em: https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/international-cooperation-cooperation-other_pt. Acesso em: 09 de julho de 2022.

camadas: física, de rede e de aplicação. A camada física é responsável por captar e fornecer informações sobre o ambiente na qual se encontram inseridas[32]. A camada de rede tem a função de transmitir e processar as informações que foram coletadas pela camada física[33]. Por fim, a camada de aplicação se revela como o subconjunto de funções e serviços que são entregues ao usuário[34], ou seja, é a camada com a qual o usuário final efetivamente interage. Um estudo da *Markets and Markets*[35] prevê que o mercado de IoT industrial crescerá de 77,3 bilhões de dólares em 2020 para 110,6 bilhões em 2025 e sugere que aproximadamente 50 bilhões de dispositivos IoT serão utilizados em todo o mundo até 2030. Com estes números, é imprescindível que potências globais, como a União Europeia, transpareçam da forma mais clara possível os aspectos técnicos básicos exigidos para que seja possível alcançar a interoperabilidade dos dispositivos em seu território, de modo que tais condições técnicas não se revelem como um entrave para o mercado.

Em sequência, o documento em voga tece considerações sobre os requisitos necessários para a prosperidade do ambiente e da infraestrutura da "Internet das

32. M.M. Martín-Lopo, J. Boal, ´A. S´anchez-Miralles, A literature review of IoT energy platforms aimed at end users, Computer Networks 171 (2020), 107101, https://doi.org/10.1016/j.comnet.2020.107101 *Apud* REJEB, Abderahman. *Et al.* The big picture on the internet of things and the smart city: a review of what we know and what we need to know. *Internet of Things*, Volume 19, 2022.
33. S. Bansal, D. Kumar, IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication, International Journal of Wireless Information Networks 27 (3) (2020) 340–364, https://doi.org/10.1007/s10776-020-00483-7 *Apud* REJEB, Abderahman. *Et al.* The big picture on the internet of things and the smart city: a review of what we know and what we need to know. *Internet of Things*, Volume 19, 2022.
34. REJEB, Abderahman. *Et al.* The big picture on the internet of things and the smart city: a review of what we know and what we need to know. *Internet of Things*, Volume 19, 2022.
35. Markets and Markets. (2020). Industrial IoT (IIoT) Market by Device & Technology (Sensor, RFID, Industrial Robotics, DCS, Condition Monitoring, Networking Technology), Connectivity (Wired, Wireless, Field technology), Software (PLM, MES, SCADA), Vertical, Region - Global Forecast to 2025. https://www. marketsandmarkets.com/Market-Reports/industrial-internet-of-things-market-129733727.html?gclid=CjwKCAiA1rPyBRAREiwA1UIy8HeVQ_mbRZH2eO-FTcuZok4BdBR_57FIIK72wJX4Wg1Y1hQIuAs-cUBoCnzcQAvD_BwE *Apud* REJEB, Abderahman. *Et al.* The big picture on the internet of things and the smart city: a review of what we know and what we need to know. *Internet of Things*, Volume 19, 2022.

Coisas" no contexto europeu, assim como dedica um capítulo à introdução do tema *Human Centered IoT* (tradução livre: Internet das Coisas centrada no ser humano), onde estabelece princípios orientadores para a tecnologia de objeto do presente estudo. Uma das principais problemáticas envolvendo a infraestrutura de IoT, principalmente na camada de aplicação, diz respeito à interação entre o usuário e o dispositivo conectado, vez que os dispositivos conectados em IoT têm como principal função primária a coleta, transmissão e/ou análise de dados, de modo que a ausência de regulação específica poderia impactar inicialmente nos direitos à privacidade, o que, posteriormente, refletiria em outros direitos, a depender dos danos causados. Em contato com a camada de aplicação, o usuário teoricamente poderia exercer seu livre-arbítrio no que tange às escolhas das possibilidades e limites do tratamento de seus dados. Ocorre que, conforme sugerido por um estudo realizado por Bakows e Trossen[36], somente um ou dois a cada mil usuários optam por acessar o contrato de licença, o que revela um verdadeiro "analfabetismo" sobre os termos e condições que regem o produto com o qual o usuário irá interagir.

Conforme revelado por uma pesquisa realizada pela Comissão Europeia[37], há três crenças principais que levam o usuário a não ler os documentos legais relacionados ao produto que irá interagir: uma sobre os custos; uma normativa; e uma de controle. A primeira indica que os usuários entendem que o "custo" da leitura do documento é muito alto[38], vez que geralmente são demasiadamente longos e complexos[39], além

36. Bakows, Y., F. Marotta-Wurgler & D.R. Trossen (2009). *Does anyone read the fine print? A test of the informed minority hypothesis using clickstream data*. New York University School of Law Working Paper *Apud* European Comission. *Study on consumers' atitudes towards Terms and Conditions*, 2016. Disponível em: https://ec.europa.eu/info/sites/default/files/terms_and_conditions_final_report_en.pdf. Acesso em: 30 de julho de 2022.
37. European Comission. *Study on consumers' atitudes towards Terms and Conditions*, 2016. Disponível em: https://ec.europa.eu/info/sites/default/files/terms_and_conditions_final_report_en.pdf. Acesso em: 30 de julho de 2022.
38. Neste contexto, o termo "custo" tem conotação de tempo perdido e carga intelectual dedicada, e não necessariamente de dinheiro ou pecúnia.
39. Plaut, V.C., & R.P. Bartlett (2011). Blind consent? A social psychological investigation of non-readership of click-through agreements. Law and Human Behavior, vol. 36(4), 293-311 *Apud Idem*.

de empregarem linguagem jurídica técnica, que dificulta a sua compreensão[40]. A segunda indica que os usuários acreditam que "ninguém lê os termos e condições"[41] e, por isso, tendem a seguir esse comportamento[42]. A última revela que há uma crença amplamente difundida na qual se você quer utilizar determinado programa ou adquirir determinado produto, não tem escolha a não ser aceitar os termos e condições da forma como estão redigidos, ou seja, os usuários acreditam que não há sentido em ler o documento, vez que não possuem o poder de alterá-los[43].

Diante deste contexto, é revelado que o mercado, grosso modo, não dedica uma atenção especial ao seu usuário no que tange à efetiva possibilidade de garantir a ciência e o exercício de seus direitos, se limitando a cumprir uma exigência legal de confeccionar o documento, sem se preocupar com a sua real usabilidade. O documento da Comissão Europeia em análise busca reverter este cenário, ao passo em que coloca a figura do ser humano no centro da tecnologia, ou seja, a regulação europeia se preocupa efetivamente com a interpretação e à garantia de oportunidade ao cidadão para que exerça seus direitos.

Por fim, o documento traz em seu anexo importantes considerações sobre as áreas que terão maior impacto direto com a implantação da "Internet das Coisas" em seu contexto, quais sejam: casas inteligentes (*smart homes)*, bem-estar pessoal e "vestíveis" (*personal wellness and wearables*), fabricação inteligente (*smart manufacturing*), energia inteligente (*smart energy*), cidades inteligentes (*smart cities*), mobilidade inteligente e automação veicular (*automated driving and smart mobility*), agricultura inteligente (*smart farming*) e economia circular (*circular economy*).

Portanto, verifica-se que, em menos de 20 anos, a União Europeia saiu de um marco inicial no qual citava o termo "Internet das Coisas" de forma tímida e incipiente, com considerações superficiais (*Comission staff working paper i2010*), para uma

40. Hartley, J. (2000). Legal ease and 'legalese'. *Psychology, Crime and Law*, vol. 6(1–2), 1–20 *Apud Idem*.

41. Plaut, V.C., & R.P. Bartlett (2011). Blind consent? A social psychological investigation of non-readership of click-through agreements. *Law and Human Behavior*, vol. 36(4), 293-311 *Apud Idem*.

42. E.g., Cialdini, R. (2001). Influence: Science and Practice. Boston: Allyn & Bacon *Apud Idem*.

43. Hillman, R. A., & J.J. Rachlinski (2002). Standard-form contracting in the electronic age. *New York University Law Review*, vol. 77, 429–495 *Apud Idem*.

série de regulações específicas, dedicadas integralmente ao tema (dentre elas, o *Commission staff working document – Advancing the Internet of Things in Europe*). Do estudo realizado, depreende-se que a União Europeia se encontra em um estágio regulatório avançado sobre o tema, próximo à conformidade com o estado de avanço da tecnologia no bloco, levando em consideração, principalmente, a quantidade e especificidade das normas existentes, o conteúdo dos documentos envolvidos na regulação (contendo aspectos técnicos, jurídicos e transdisciplinares), assim como a quantidade de grupos de cooperação internacional na qual o bloco participa ativamente em matéria de privacidade e proteção de dados.

4. PERSPECTIVAS PARA O FUTURO DA REGULAÇÃO DA IOT NO BRASIL

Conforme se depreende da leitura dos tópicos acima, em que pese a tecnologia da "Internet das Coisas" ser algo extremamente recente em termos históricos, é possível verificar que o Brasil já reconheceu a sua importância, assim como o Governo Federal já deu o primeiro passo em direção à sua regulação (vide o Plano Nacional de Internet das Coisas, analisado anteriormente).

Outro ponto relevante que merece destaque é o fato de o Decreto indicado não ter sido publicado com mero viés descritivo e independente de pesquisas anteriores, vez que, para que o Plano fosse efetivamente elaborado, foram realizados profundos estudos prévios, divididos em quatro fases principais[44] ao longo de dois anos, dos quais resultaram diversos documentos[45] que fundamentaram as ações estratégicas[46]

44. Veja as fases do estudo prévio à publicação do Plano Nacional de IoT em: *Estudo de Internet das Coisas*. Ministério da Ciência, Tecnologia e Inovações. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas-estudo. Acesso em: 10 de julho de 2022.
45. Veja os documentos gerados a partir dos estudos indicados em: *Estudo de Internet das Coisas*. Ministério da Ciência, Tecnologia e Inovações. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas-estudo-repositorio. Acesso em: 10 de julho de 2022.
46. Veja as ações estratégicas provenientes do estudo prévio ao Plano Nacional de IoT em: *Ações estratégicas*. Ministério da Ciência, Tecnologia e Inovações. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/nternet-das-coisas-

a serem tomadas em âmbito nacional.

Entretanto, em que pese o Governo Federal ter demonstrado interesse no tema e transparecido sua preocupação com a sua tutela e consequências, é possível verificar que o Brasil ainda não se encontra no mesmo estágio regulatório que o da União Europeia. Em realidade, no próprio contexto europeu, mesmo levando em consideração as 1.015 (mil e quinze) normas que se referem expressamente ao tema, verifica-se que a regulação no bloco indicado também ainda não chegou no mesmo patamar em que a tecnologia necessitaria para uma tutela coerente ante o seu estágio de desenvolvimento, vez que ainda restam em aberto importantes discussões envolvendo responsabilidade civil[47], propriedade intelectual[48], privacidade e proteção de dados[49], entre outras.

Essas discussões serão objetos de um futuro estudo. Para fins de conclusão deste capítulo, basta reconhecer que relevantes países e blocos econômicos[50] no contexto internacional já estão se movimentando com a finalidade de tutelar a "Internet das Coisas", e o mais importante: buscando harmonizar os direitos individuais (como a privacidade e a proteção de dados) com os interesses coletivos (como a livre circulação dos dados e a livre concorrência). Para o avanço da regulação nacional, é possível basear-se em casos de sucesso no ambiente europeu[51], que já conta com um histórico

acoes. Acesso em: 10 de julho de 2022.

47. Um exemplo desta problemática, ainda não resolvida em âmbito nacional ou internacional, seria: como tutelar a responsabilidade de um dispositivo cujo serviço foi projetado no "país 1", foi manufaturado no "país 2" e foi distribuído para venda no "país 3", sendo que cada um de seus componentes, por sua vez, veio de determinado país, com regulação própria?
48. No âmbito da propriedade intelectual, é possível se deparar com problemáticas envolvendo a burocracia e os altos custos de licenciamento de tecnologias e procedimentos registrados nos órgãos nacionais de cada localidade.
49. Discussões como: qual o limite entre a proteção de dados (interesses do particular) e a livre concorrência e a livre circulação dos dados (interesses mercadológicos), no que tange à coleta, armazenamento e compartilhamento de dados pelos dispositivos conectados em IoT.
50. O termo "relevantes" foi utilizado por se tratar de países/blocos com grande influência política e econômica no contexto internacional.
51. Veja um relatório de *benchmarking* proveniente do estudo prévio ao Plano Nacional de IoT em: *Benchmark de iniciativas e políticas públicas*. Governo Federal. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinternetdascoisas/fase1_1_relatorio-de-benchmark.pdf. Acesso em: 10 de julho de 2022.

mais amplo e consolidado sobre a regulação do tema.

Como sugestões provenientes do presente estudo comparativo, foram escolhidos dois conceitos para auxiliar o avanço nacional neste sentido: *Single market for the IoT* (tradução livre: "mercado único para a IoT") e *Human Centered IoT* (tradução livre: "IoT centrada no ser humano"). Ambos os conceitos indicados são trazidos por documento anteriormente já abordado neste estudo[52].

A Comissão Europeia define *Single market for the IoT* como "a capacidade de os dispositivos serem capazes de se conectar perfeitamente e de forma *plug-and-play* em qualquer local na União Europeia e expandir além das fronteiras"[53]. Na prática, trata-se do estabelecimento de premissas universais entre os países-membros no que tange à conectividade, numeração, endereçamento, redes de telecomunicações, fluxos de dados e responsabilidades. Tal conceito poderia ser importado, por exemplo, de forma que o Mercosul adotasse premissas universais entre os países-membros, assim como a União Europeia, de modo a, no futuro, facilitar uma eventual expansão da regulação para além das fronteiras dos blocos econômicos, visando uma verdadeira "regulação global para o cenário de IoT". Afinal, a principal premissa da "Internet das Coisas" é a conectividade, independente de fronteiras geopolíticas.

Já o termo *Human Centered IoT* é definido como "a necessidade de a Internet das Coisas respeitar os valores europeus, capacitando pessoas, máquinas e empresas graças a altos padrões de proteção de dados pessoais e segurança"[54]. Na prática, trata-se da preocupação com que as soluções de IoT sejam desenvolvidas tendo por premissa os direitos individuais do ser humano, o que pode ser feito, por exemplo, observando

52. *COMMISSION STAFF WORKING DOCUMENT Advancing the Internet of Things in Europe*. EUR-Lex. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110. Acesso em: 09 de julho de 2022.

53. *Idem*.

54. *Idem*.

frameworks de segurança como o COBIT[55] e o ISO/IEC 38500[56] ou mesmo realizando pesquisas de campo diretamente com os usuários[57]. Tal conceito poderia ser importado, por exemplo, de modo que fosse realizada uma pesquisa de âmbito nacional sobre como os usuários/consumidores brasileiros interagem com os documentos e termos provenientes dos produtos e serviços de IoT, verificando o seu grau de compreensão e o nível de maturidade da população quanto à sua interpretação e avaliação de riscos. Uma vez realizado este levantamento inicial, poderiam ser estabelecidos parâmetros regulatórios de observação vinculante para as empresas (produtoras/fornecedoras de soluções de IoT) em âmbito nacional (ou, quem sabe, em âmbito transnacional) para que utilizassem técnicas[58] garantidoras de uma compreensão ao menos básica sobre o assunto, de acordo com o seu nível de potencial risco e gravidade.

Dessa forma, é possível vislumbrar um horizonte onde a tecnologia da "Internet das Coisas" alcança uma conectividade transnacional, alcançando seus objetivos mercadológicos e, ao mesmo tempo, respeitando os direitos e valores humanos.

5. CONCLUSÃO

Em que pese a "Internet das Coisas" ser uma tecnologia relativamente recente em

55. Controle de Objetivos para Informação e Tecnologias. Trata-se de um recurso que objetiva auxiliar gerentes de TI no controle e no cumprimento de seus objetivos, mantendo-os alinhados com os objetivos da organização. LUCIANO, Edimara Mezzomo; TESTA, Mauricio Gregianin. *Controles de governança de tecnologia da informação para a terceirização de processos de negócio: uma proposta a partir do COBIT*. JISTEM - Journal of Information Systems and Technology Management, 2011.
56. Norma que fornece princípios, definições e um modelo para os órgãos governamentais usarem ao avaliar, dirigir e monitorar o uso da tecnologia das informações em suas organizações. *ISO/IEC 38500:2015*. ISO. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en. Acesso em: 10 de julho de 2022.
57. *Study on consumers' atitudes towards Terms and Conditions (T&Cs)*. European Commission. Disponível em: https://ec.europa.eu/info/sites/default/files/terms_and_conditions_final_report_en.pdf. Acesso em: 10 de julho de 2022.
58. Sobre o tema, diversas técnicas com este fim são desenvolvidas na área do Legal Design. FALEIROS JÚNIOR, José L. M.; CALAZA, Tales. *Legal design: teoria e prática*. Indaiatuba: Editora Foco. 2021.

termos históricos, as suas implicações remontam a debates iniciados no século XIX, por Samuel D. Warren e Louis D. Brandeis[59], no que tange à privacidade e à proteção de dados pessoais.

Diante das inúmeras consequências que tal infraestrutura e os dispositivos a ela conectados podem refletir no âmbito civil e constitucional, diversos países e blocos econômicos estão em busca de sua regulação, de modo que atendam os interesses mercadológicos e garantam os direitos individuais dos usuários, sem que se traduzam como um empecilho para a inovação.

A União Europeia se revela na vanguarda da regulação desta tecnologia, vez que as normas oficiais que fazem menção expressa ao tema remontam ao ano de 2006, sendo que o bloco conta hoje com nada menos do que 1.015 normas oficiais, que ao menos tangenciam essa tecnologia.

O Brasil, em que pese ter iniciado seu caminho regulatório de forma mais recente, já demonstrou preocupação com o tema e as ações estratégicas desenvolvidas pelo Governo Federal apontam para um horizonte onde a regulação será mais robusta e completa.

Para que este horizonte seja alcançado de forma breve e coerente, é possível importar modelos de sucesso já discutidos ou efetivamente implementados em outros locais de referência, como a própria União Europeia. De início, sugere-se a aplicação dos conceitos *Single market for the Iot* e *Human Centered IoT* em âmbito nacional, para que, posteriormente, sejam desenvolvidos novos debates sobre a regulação da IoT em conjunto com outros países e blocos econômicos.

REFERÊNCIAS

BRASIL. *Constituição (1988)*. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. *Decreto nº 10.222/2020 (Estratégia Nacional de Segurança Cibernética)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 10 de julho de 2022.

59. WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1. Acesso em: 09 de julho de 2022.

BRASIL. *Decreto nº 10.463/2020*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10463.htm. Acesso em: 10 de julho de 2022.

BRASIL. *Decreto nº 9.637/2018 (Política Nacional de Segurança da Informação)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art6i. Acesso em: 10 de julho de 2022.

BRASIL. *Decreto nº 9.854/2019 (Plano Nacional de Internet das Coisas)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9854.htm. Acesso em: 10 de julho de 2022.

BRASIL. Governo Federal. *Benchmark de iniciativas e políticas públicas*. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinternetdas-coisas/fase1_1_relatorio-de-benchmark.pdf. Acesso em: 10 de julho de 2022.

BRASIL. Legislação Federal Brasileira. *"Internet das Coisas"*. Disponível em: https://legislacao.presidencia.gov.br/#. Acesso em: 10 de julho de 2022.

BRASIL. *Lei nº 12.965/2014 (Marco Civil da Internet)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 09 de julho de 2022.

BRASIL. *Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09 de julho de 2022.

BRASIL. *Lei nº 8.078/1990 (Código de Defesa do Consumidor)*. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 09 de julho de 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. *Ações estratégicas*. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/nternet-das-coisas-acoes. Acesso em: 10 de julho de 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. *Estratégia brasileira para a transformação digital (E-Digital)*. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/estrategia-digital. Acesso em: 30 de julho de 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. *Estudo de Internet das Coisas*. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas-estudo. Acesso em: 10 de julho de 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. *Estudo de Internet das Coisas*. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas-estudo-repositorio. Acesso em: 10 de julho de 2022.

CALAZA, Tales. *O direito à privacidade: origem histórica e jurídica*. *In:* LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura; BORGES, Gabriel de Oliveira Aguiar; REIS, Guilherme (Coords.). *Fundamentos do direito digital*. Uberlândia: LAECC, 2020, pp. 169-183.

Comission staff working paper – i2010 – First Annual Report on the European Information Society {COM(2006)215}. EUR-Lex. Disponível em: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=CELEX%3A52006SC0604&qid=1657396829302. Acesso em: 09 de julho de 2022.

COMMISSION STAFF WORKING DOCUMENT Advancing the Internet of Things in Europe. EUR-Lex. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110. Acesso em: 09 de julho de 2022.

CONGRESSO NACIONAL. Projeto plurianual da União para o período de 2016 a 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=C93FBE24E28C7EAF229B4AD8E0AB8BBC.proposicoesWeb1?codteor=1426481&filename=Tramitacao-PLN+6/2015+CN. Acesso em: 31 de julho de 2022.

DICIO. Dicionário Online de Português. *Regulação*. Disponível em: https://www.dicio.com.br/regulacao/. Acesso em: 09 de julho de 2022.

DICIO. Dicionário Online de Português. *Regular*. Disponível em: https://www.dicio.com.br/regular/. Acesso em: 09 de julho de 2022.

EUROPA. Council of Europe. *Details of Treaty No. 108*. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 09 de julho de 2022.

EUROPA. EUR-Lex. *"Internet of things"*. Disponível em: https://eur-lex.europa.eu/search.html?lang=en&text=%22internet+of+things%22&qid=1657396829302&type=quick&scope=EURLEX. Acesso em: 09 de julho de 2022.

EUROPA. EUR-Lex. *Regulamento (UE) 2016/679*. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A32016R0679. Acesso em: 09 de julho de 2022.

EUROPA. European Comission. *Staff Working Document: Advancing the Internet of Things in Europe*. 2016. Disponível em: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-advancing-internet-things-europe. Acesso em: 05 de julho de 2022.

EUROPA. European Comission. *Study on consumers' atitudes towards Terms and Conditions (T&Cs)*. Disponível em: https://ec.europa.eu/info/sites/default/files/terms_and_conditions_final_report_en.pdf. Acesso em: 10 de julho de 2022.

EUROPA. European Commission. *Study on consumers' atitudes towards Terms and Conditions*, 2016. Disponível em: https://ec.europa.eu/info/sites/default/files/terms_and_conditions_final_report_en.pdf. Acesso em: 30 de julho de 2022.

EUROPA. European Data Protection Board. *Cooperação internacional*. Disponível em: https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/international-cooperation-cooperation-other_pt. Acesso em: 09 de julho de 2022.

EUROPA. European Parliament. *Proteção de dados pessoais*. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 09 de julho de 2022.

EUROPA. Parlamento Europeu. *Directiva 95/46/CE do Parlamento Europeu e do Conselho*. EUR-Lex. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 09 de julho de 2022.

FALEIROS JÚNIOR, José L. M.; CALAZA, Tales (Coord.). *Legal design*: teoria e prática. Indaiatuba: Editora Foco. 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 38500:2015*. ISO. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en. Acesso em: 10 de julho de 2022.

KITAMURA, Celso. *Faça sua lista de compras com a Alexa*. Celso Kitamura, 2021. Disponível em: https://celsokitamura.com.br/faca-sua-lista-de-compras-com-a-alexa/. Acesso em: 05 de julho de 2022.

LACERDA, Flávia. *Análise ex ante do plano nacional de Internet das Coisas (IoT):* ambiente cidades inteligentes. Instituto Serzedello Corrêa, 2020.

LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. *Revista do Direito*, n. 30, p. 138-160, 15 jul. 2008.

LUCIANO, Edimara Mezzomo; TESTA, Mauricio Gregianin. Controles de governança de tecnologia da informação para a terceirização de processos de negócio: uma proposta a partir do COBIT. *Journal of Information Systems and Technology Management*, 2011.

MATTERE, Henrique. Casa automatizada – Como acender luz pelo celular? *Mundo da Elétrica*. Disponível em: https://www.mundodaeletrica.com.br/casa-automatizada-como-acender-luz-pelo-celular/. Acesso em: 05 de julho de 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Os objetivos de desenvolvimento sustentável no Brasil*. Disponível em: https://brasil.un.org/pt-br/sdgs. Acesso em: 04 de agosto de 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais*. OECD. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 09 de julho de 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Revisão do Governo Digital do Brasil: rumo à transformação digital do setor público*. Disponível em: https://repositorio.enap.gov.br/bitstream/1/3627/1/2b.%20Review%20OCDE%20Governo%20Digital%20%28Portugu%C3%AAs%29.pdf. Acesso em: 30 de julho de 2022.

REJEB, Abderahman *et al*. The big picture on the internet of things and the smart city: a review of what we know and what we need to know. *Internet of Things*, Volume 19, 2022.

SYNERGY CONSULTING. *Enabling the IoT ecosystem with a policy and regulation*. Disponível em: https://www.synergyconsulting.ae/insights/enabling-iot-ecosystem-policy-regulation/. Acesso em: 05 de julho de 2022.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge,

v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1. Acesso em: 09 de julho de 2022.

A PROPOSTA DE REGULAÇÃO DA IA NO BRASIL E POSSÍVEIS IMPACTOS PARA A INTERNET DAS COISAS:
REFLEXÕES INICIAIS

Marcela Mattiuzzo

Doutoranda em Direito Comercial na Universidade de São Paulo, pela qual também é Mestra em Direito Constitucional. Coordenadora do Núcleo de Direito Concorrencial e Economia Digital (Nuced) da Faculdade de Direito da USP e sócia de VMCA Advogados. Foi pesquisadora visitante na Yale Law School (2016-2017), Chefe de Gabinete e Assessora da Presidência do Conselho Administrativo de Defesa Econômica (2015-2016). É autora de textos sobre concorrência, regulação e mercados digitais.

Flávia Parra Cano

Graduanda em Direito na Universidade de São Paulo com ênfase em teoria do direito, direito digital, proteção de dados e direitos humanos. Foi bolsista no PET (Programa de Educação Tutorial) - Sociologia Jurídica sob a tutoria do Professor Associado Rafael Mafei Rabelo Queiroz, no qual desenvolveu Iniciação Científica em direito urbanístico, apresentada no IX EPED.

DOI: https://doi.org/10.59224/dti5.ch2

Resumo: Nos últimos anos, a Internet das Coisas (IoT) tem desempenhado um papel significativo na transformação da sociedade. Dispositivos inteligentes conectados à internet estão cada vez mais presentes no cotidiano. Grandes empresas, como Google e Amazon, lançaram assistentes virtuais baseados em IoT, como o Google Home e a Alexa, impulsionando o crescimento desse mercado. No entanto, questões surgem em relação à propriedade e uso dos dados gerados pela IoT, bem como a privacidade e segurança dos dados pessoais coletados. A Lei Geral de Proteção

Abstract: *In recent years, the Internet of Things (IoT) has played a significant role in transforming society. Smart devices connected to the internet are increasingly present in our daily lives, encompassing areas such as healthcare, smart homes, and smart cities. Major companies like Google and Amazon have launched IoT-based virtual assistants such as Google Home and Alexa, driving the growth of this market. However, concerns arise regarding the ownership and use of data generated by IoT, as well as the privacy and security of collected personal data. The General Data Protection Law (LGPD) in*

de Dados Pessoais (LGPD) no Brasil tenta regular essas questões, mas a aplicação da legislação nesse contexto é desafiadora. Além disso, o Anteprojeto de lei de inteligência artificial no país também pode impactar o desenvolvimento da IoT. O objetivo deste artigo é explorar de forma preliminar como o Anteprojeto poderia afetar a IoT, abordando temas relevantes relacionados à regulamentação e aplicação da tecnologia.
Palavras-chave: Inteligência Artificial; Internet das Coisas; regulação.

Brazil attempts to regulate these issues, but its application in this context is challenging. Additionally, the draft law on artificial intelligence in the country may also impact the development of IoT. The objective of this article is to explore, in a preliminary manner, how the draft law could affect IoT, addressing relevant topics related to regulation and application of the technology.

Keywords: *Artificial Intelligence; Internet of Things; regulation.*

1. INTRODUÇÃO

Na última década, uma série de inovações no campo tecnológico tem mudado a maneira como se pensa na interação da sociedade com a tecnologia, sendo que diversas dessas inovações têm se mostrado especialmente transformadoras e cada vez mais presentes em nosso cotidiano. Um dos principais motores de tal transformação vem, justamente, da expansão do uso da Internet das Coisas (ou IoT, na sigla em inglês que se refere a Internet of Things) no dia a dia, por conta da presença mais frequente de dispositivos e aparelhos denominados "inteligentes" (expressão que, normalmente, diz respeito à capacidade de tais instrumentos se conectarem à *internet* e às outras redes de comunicação, trocando e/ou gerando informações a partir de sensores ou com base no uso de *softwares*, por exemplo). Na definição da

Organização para Cooperação e Desenvolvimento Econômico ("OCDE"), a IoT se refere justamente a esse ecossistema em que aplicativos e serviços são fundamentados na coleta de dados por meio de dispositivos que se colocam como interface no mundo físico.[1]

Nesse contexto, se, anteriormente, já estávamos mais habituados aos *notebooks* e aos *smartphones* como exemplos de tecnologias conectadas, o que tem ocorrido atualmente é a expansão da conexão à rede a dispositivos diversos, como televisões, aparelhos domésticos e de iluminação (no âmbito doméstico ou nas ruas), veículos, dispositivos como *smartwatches* e outros.[2] Algumas das maiores empresas de tecnologia, como Google e Amazon, já lançaram dispositivos que funcionam como assistentes virtuais (Google Home e Alexa, respectivamente) e usam a IoT para diversas funcionalidades.[3] A respeito da Amazon, inclusive, dados recentes mostram que, só em 2021, as interações dos usuários com a Alexa aumentaram em 30%, reforçando o crescimento deste mercado.[4]

Essas mesmas empresas, inclusive, têm expandido as suas aquisições relacionadas ao mercado de IoT, como demonstra a aquisição do Fitbit, focado no desenvolvimento de *smartwatches,* pelo Google, realizada no valor de pouco mais de dois bilhões de dólares.[5] A medida veio como uma tentativa do Google de se firmar no

1. Organização para Cooperação e Desenvolvimento Econômico (OECD). The Internet Of Things: Seizing the Benefits and Addressing the Challenges (Background report for Ministerial Panel 2.2). Working Party on Communication Infrastructures and Services Policy. Paris: OCDE, 2016. p. 5. Disponível em: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En.
2. YOO, Christopher S. The Emerging Internet of Things Opportunities and Challenges for Privacy and Security. In: Governing Cyberspace during a Crisis in Trust. Centre for International Governance, 2019. p. 41. Disponível em: https://www.cigionline.org/articles/emerging-internet-things/.
3. Ibid. p. 41.
4. PETERS, Jay. Amazon is subjecting Alexa to a performance review: The Wall Street Journal reports that Alexa is one of the company's businesses under scrutiny as part of a cost-cutting review led by CEO Andy Jassy. The Verge, 2022. Disponível em: https://www.theverge.com/2022/11/10/23451534/amazon-alexa-cost-cutting-review-andy-jassy.
5. SATARIANO, Adam; WAKABAYASHI, Daisuke. Google to Buy Fitbit for $2.1 Billion: The deal represents an aggressive attempt by Google to bolster its lineup of hardware products. The New York Times, 2019. Disponível em: https://www.nytimes.com/2019/11/01/technology/google-

mercado de *wearables* baseados em IoT, o qual era marcado por forte predominância da Apple em razão da comercialização do Apple Watch, o *smartwatch* da empresa. A aquisição da Fitbit pelo Google foi, inclusive, alvo de investigação por parte da Comissão Europeia e de outras autoridades mundo afora do ponto de vista concorrencial, já que se considerou que poderia prejudicar a concorrência no mercado de *wearables*.[6] A partir desse exemplo, percebe-se que o mercado relacionado à IoT de fato tem se expandido nos últimos anos, crescendo em valor agregado e participação de empresas, especialmente de tecnologia.

Além disso, pode-se notar que a aplicação de IoT normalmente é mais observada (e sentida) em alguns setores específicos, ainda que possa ser empregada em qualquer área, considerando que, como destacado, essa tecnologia diz mais respeito a uma determinada forma de conectividade entre redes, como a *internet*, e dispositivos para a coleta de informações, do que a um determinado setor, produto ou serviço.

De toda forma, dentre os setores principais em que se vê claramente a aplicação de IoT, destacam-se a área da saúde (por meio de *wearables*, inclusive), aplicação no âmbito doméstico (por meio de dispositivos que costumam ser agregados sob a nomenclatura de *smart homes*) e também nas *smart cities* (a ideia de cidades inteligentes, ou seja, ambientes urbanos embebidos em tecnologias e em dispositivos que se pautem em IoT para coletar dados e tornar os ambientes mais eficientes para cidadãos e negócios).[7]

Há diversas aplicações de IoT em relação às quais não necessariamente existem implicações relevantes de um ponto de vista de dados pessoais, ou seja, casos de uso em que não ocorre a coleta de informações relacionadas às pessoas físicas (ex.: usos na agricultura ou na indústria, nos quais se pode coletar dados relacionados a uma

---

fitbit.html.

6. A Comissão Europeia terminou aprovando a aquisição no ano de 2020. PODESTA, Arianna; TSONI, Maria. Commission clears acquisition of Fitbit by Google, subject to conditions. Comissão Europeia, 2020. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.
7. COMISSÃO EUROPEIA. What are smart cities: Cities using technological solutions to improve the management and efficiency of the urban environment. Disponível em: https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

determinada máquina ou plantação), ou no mínimo em que essa coleta não ocorre de forma relevante.

No entanto, é frequente (e em boa medida esperado) que os questionamentos e as principais dúvidas em termos de uso e aplicação de IoT surjam, especialmente, quando há o envolvimento de dados pessoais[8] para desenvolvimento dos dispositivos. Assim, ainda que prometam um aumento de eficiência, benefícios para a sociedade e negócios, junto ao uso de dispositivos IoT aparecem discussões complexas: de quem são os dados e as informações gerados a partir da aplicação de IoT, para quais finalidades serão utilizados, como poderemos garantir mais transparência em relação ao tratamento de dados pessoais gerados por IoT, quais as medidas de segurança que devem ser adotadas a fim de proteger as pessoas (e, mais especificamente, os titulares de dados, quando esse conceito for aplicável), dentre diversas outras.[9]

Nessa toada, há um debate relevante que trata das características dos dados coletados por meio da IoT. Isso porque, em diversos casos, os dados coletados por tais dispositivos parecem, com base em uma análise preliminar, triviais do ponto de vista das pessoas físicas.[10] No entanto, esses mesmos dados podem vir a ser utilizados, em um momento posterior, de modo a descobrir *insights* granulares e até mesmo íntimos a respeito das pessoas que foram alvo da coleta das informações.[11] Em especial, o que vale destacar é que a IoT permite que informações anteriormente não tidas como dados pessoais (ex.: dados sobre os produtos que abastecem uma geladeira) possam ser recombinados com a finalidade de identificar indivíduos e obter informações mais específicas sobre eles, que poderão, por sua vez, ser consideradas como dados pessoais (ex.: os dados a respeito de consumo ou mesmo dados de saúde

8. Dados pessoais, quando mencionados, serão aqui definidos nos termos do art. 5º, I, da Lei nº 13.709/2018 (a Lei Geral de Proteção de Dados). O mesmo será aplicável a outros termos definidos na referida legislação.
9. PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. Austin: Texas Law Review, 2014. p. 5. Disponível em: https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf.
10. EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Durham: Duke Law & Technology Review, v. 18, 2017. p. 34-35. Disponível em: https://scholarship.law.duke.edu/dltr/vol16/iss1/2/.
11. Ibid. p. 34.

relacionados à alimentação de uma família após inferências).[12]

Quando pensamos na intersecção entre IoT e proteção de dados pessoais, é inevitável que, no Brasil, sejamos instados a analisar a Lei nº 13.709/2018 (a Lei Geral de Proteção de Dados Pessoais ou "LGPD"). Mas, como dito, a complexidade dos temas envolvidos no uso de IoT e dos próprios dispositivos que a utilizam tornam a discussão e a aplicação da LGPD (e de outras legislações referentes à proteção de dados pessoais) desafiadora. Isso porque, em diversos casos, pensar em IoT e tratamento de dados pessoais significa pensar fora da lógica pré-estabelecida por parte desse arcabouço legislativo. No exemplo acima da geladeira inteligente, imaginando que se trata de eletrodoméstico utilizado por uma família composta por dois adultos e duas crianças, como identificar a quem pertence cada dado coletado? Caso a inferência de dados de saúde de fato ocorra, de que maneira seria possível identificar qual o titular de dados cujas informações podem ser inferidas de modo adequado? No caso em tela, isso seria especialmente relevante tendo em vista que a LGPD estabelece um regime diferente para o tratamento de dados pessoais de crianças e adolescentes, mais protetivo, de modo geral, quando o comparamos com o regime geral da lei.

A LGPD, em um sentido muito geral, estabelece uma lógica para as atividades de tratamento praticamente linear: há um controlador de dados pessoais (ou um conjunto de controladores), o qual decide realizar uma atividade de tratamento a partir da coleta de dados pré-definidos para certas finalidades também pré-estabelecidas. É possível também existir um operador, que realiza o todo ou parte da atividade de tratamento em nome do controlador. Para realizar o tratamento em conformidade com a lei, os agentes teriam de respeitar as demais obrigações legais, especialmente as relacionadas aos direitos dos titulares sobre o tratamento de dados e à transparência quanto às próprias atividades de tratamento, as quais devem estar claras aos titulares por elas impactados.

Portanto, a LGPD auxilia justamente a ilustrar que determinadas regulações podem impactar o desenvolvimento de IoT de forma relevante, tendo em vista as características de tal tecnologia. A partir dessa constatação, pode-se questionar quais outras regulações poderiam afetar a IoT como tecnologia e mercado em expansão no Brasil.

12. Ibid. p. 35.

Nesse sentido, um dos marcos regulatórios de maior impacto que tem sido discutido na área de tecnologia no país é o Anteprojeto de lei de inteligência artificial ("Anteprojeto"), que advém do trabalho desenvolvido pela Comissão de Juristas Responsável por Subsidiar Elaboração De Substitutivo Sobre Inteligência Artificial No Brasil ("CJSUBIA"), instaurada por parte do Senado Federal no início de 2022.[13] O movimento brasileiro segue as principais discussões que também têm ocorrido na União Europeia ("UE") quanto ao tema da inteligência artificial ("IA"), sendo que o Conselho da União Europeia apresentou recentemente sua versão final do chamado *AI Act*, a proposta da UE de regulação de IA.[14]

Por conseguinte, seguindo o pensamento de que regulações que impactem aspectos do funcionamento de IoT podem terminar por afetar o desenvolvimento deste campo, o objetivo deste artigo é pensar, de forma preliminar, como o Anteprojeto poderia ter reflexos para a internet das coisas. Para isso, a intenção é abordarmos, ao longo das próximas páginas, alguns (e certamente não todos) dos temas que figuram no Anteprojeto e que seriam relevantes quando pensamos especificamente na sua aplicação à IoT.

2. A COMPLEXIDADE DE REGULAR A IOT E A RELEVÂNCIA DO ANTEPROJETO

Compreender os possíveis impactos do Anteprojeto para a IoT é relevante se pensarmos que pode haver uma tendência de que dispositivos que fazem uso de IoT implementem sistemas algorítmicos de inteligência artificial.

Como já posto acima, o mercado de IoT tem se expandido de forma constante. Junto a ele, um outro mercado cada vez mais relevante no âmbito da tecnologia é justamente o de IA. Conforme relatório do US Commercial Services, parte do US Department of Commerce, órgão do governo dos Estados Unidos, o investimento em IA, a nível global, chegou a cerca de sessenta e sete bilhões de dólares em 2021, sendo que, nesse mesmo ano, sessenta e cinco empresas focadas no desenvolvimento

13. O objetivo central era propor um texto substitutivo aos PLs nº 872/2021, nº 21/2020 e nº 5.051/2019.

14. A versão do *AI Act* proposta pelo Conselho da União Europeia pode ser encontrada no seguinte *link*: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf.

de IA tiveram o seu valor de mercado avaliado em mais de um bilhão de dólares.[15] Especificamente em relação ao Brasil, levantamento do Google mostrou que mais de dois bilhões de dólares investidos em IA na América Latina foram direcionados ao país no ano de 2020, havendo um aumento de *startups* focadas em IA no território brasileiro.[16]

Assim, é inquestionável a relevância dos mercados de IoT e IA, separadamente, na área de tecnologia (e em outros segmentos que utilizem essas tecnologias). Existe também, nesse contexto, a possibilidade de se desenvolver dispositivos de IoT que façam de IA.[17] Isso porque, enquanto a IoT facilita especialmente a coleta de dados (pessoais ou não), a IA pode auxiliar a analisar esses dados de forma mais eficiente, o que torna a junção de tais tecnologias desejável para o desenvolvimento de produtos e serviços. Dentre os aspectos que sustentam essa perspectiva, por exemplo, podemos citar que as aquisições de *startups* que desenvolvem IoT com uso de IA estão em alta e que fornecedores de IoT, tais como Amazon, IBM, Microsoft e Oracle, estão incluindo elementos de IA em diversos de seus produtos.[18]

Se a própria conceituação de IA e IoT é desafiadora, na medida em que diversos autores defendem que em especial a inteligência artificial não é propriamente uma tecnologia, mas sim um conjunto de tecnologias que comporta facetas bastante diversas, e também que a sua aplicação pode se dar num universo extremamente amplo de setores e segmentos - ou seja, não estamos diante de uma tecnologia de uso específico, com relevância para a área da saúde, por exemplo, mas sim de possíveis aplicações em absolutamente todos os segmentos, para as mais diversas finalidades, que incluem desde o gerenciamento dos recursos humanos de uma empresa até a criação

15. US COMMERCIAL SERVICE. Top Global Artificial Intelligence Markets Report. Department of Commerce of the United States of America, 2021. p. 2. Disponível em: https://www.trade.gov/sites/default/files/2022-05/Top%20Global%20AI%20Markets%20Report%204.20%20%282%29%20%281%29.pdf.
16. ABSTARTUPS; BOX 1824; GOOGLE FOR STARTUPS. O impacto e o futuro da Inteligência Artificial no Brasil. 2022. p. 7. Disponível em: https://drive.google.com/file/d/1ETBrrCfpnaviNY3z8eQX3cXHNe7iq7uF/view.
17. SCHATSKY, David, KUMAR, Navya, BUMB, Sourabh. Bringing the Power of AI to the Internet of Things. The Wired. Disponível em: https://www.wired.com/brandlab/2018/05/bringing-power-ai-internet-things/.
18. Ibid.

de obras de arte - o nível de complexidade só aumenta se pensamos em seu uso conjunto.

Assim, a união de IoT e IA em dispositivos e aplicações gera, inegavelmente, dúvidas regulatórias em face do Anteprojeto.[19]

Explicados o recorte do presente artigo e as razões para o enfoque no Anteprojeto, passa-se à análise mais detalhada do seu texto e de que forma ele pode impactar o desenvolvimento de IoT enriquecido por IA.

3. A ANÁLISE DA POSSÍVEL APLICAÇÃO DO ANTEPROJETO DE LEI DE IA À IOT

O mercado de IoT plenamente conjugado com IA ainda não é uma realidade. De toda forma, como visto acima, elementos concretos permitem concluir que este é um provável passo no ramo de desenvolvimento da tecnologia, o qual, como ocorrido com IoT e IA separadamente, pode se espalhar rapidamente por diversos aspectos do cotidiano e se expandir, inclusive, aos cenários já comuns nos quais observamos a presença de dispositivos que utilizam IoT.[20] Assim, uma vez superados os obstáculos técnicos para que IA e IoT funcionem plenamente em conjunto, a tendência é que esse uso aumente.

Nessa conjuntura, pensando especificamente no Anteprojeto proposto pela CJSUBIA, temos uma situação a partir da qual podemos, em decorrência da regulação da IA, impactar o desenvolvimento de aplicações e dispositivos que utilizem a IA como parte de seu funcionamento, mas que sejam fundamentalmente dispositivos IoT. Sabe-se que a regulação de IA não é um assunto simples, muito menos pouco controverso, tendo em vista a complexidade do funcionamento da própria tecnologia. Assim, ao pensarmos em IA e IoT de forma conjunta, surgem ainda mais dúvidas sobre como aplicar referida regulação de maneira coerente e que, ao mesmo tempo,

19. Tal como ressaltado quanto à LGPD, os conceitos e termos definidos pelo Anteprojeto de lei de IA que forem utilizados na redação do artigo devem ser lidos conforme a definição dada pelo próprio Anteprojeto.

20. SCHATSKY, David, KUMAR, Navya, BUMB, Sourabh. Bringing the Power of AI to the Internet of Things. The Wired. Disponível em: https://www.wired.com/brandlab/2018/05/bringing-power-ai-internet-things/.

proteja os indivíduos e não apresente empecilhos intransponíveis para o desenvolvimento tecnológico.

Com base no texto do Anteprojeto, algumas das principais dificuldades que poderiam surgir como resultado do uso conjunto de IA e IoT vislumbradas inicialmente dizem respeito: **(i)** à aplicação dos direitos previstos na proposta a dispositivos de IoT que utilizem IA; **(ii)** aos possíveis impactos da classificação de riscos para fins de IA aos sistemas e dispositivos que utilizem IoT e IA em conjunto; e **(iii)** à adequação da autoridade prevista no Anteprojeto para a regulação de sistemas e dispositivos que utilizem também IoT. Para além da aplicação conjunta de IoT e IA, a análise a seguir também buscará tratar de riscos, em geral, que podem advir da aplicação de conceitos e dispositivos do Anteprojeto, pressupondo que ele seja aprovado pelo Congresso Nacional na forma como se encontra hoje.[21-22]

3.1. DIREITOS DAS PESSOAS AFETADAS

Em termos dos direitos previstos pelo Anteprojeto, vale notar, em um primeiro momento, que há desafios estruturais na sua aplicação independentemente da correlação entre IA e IoT. Nesse sentido, um ponto central é que o texto descreve que tais direitos são relacionados essencialmente às "pessoas afetadas" por sistemas de IA, de maneira bastante ampla. Porém, ainda que a ideia de pessoas afetadas apareça ao longo da redação de todos os dispositivos legais, não há uma definição mais precisa do que se entende por esse conceito – diferentemente do que ocorre com outros

21. Para fins de referência, o presente artigo foi desenvolvido com base na versão do Anteprojeto que se encontra disponível no relatório final da CJSUBIA, entregue ao Senado Federal em 06 de dezembro de 2022. Por conseguinte, as mudanças que eventualmente ocorrerem durante a sua discussão no Congresso Nacional não serão contempladas pelo artigo. O referido relatório pode ser encontrado no seguinte *link*: https://legis.senado.leg.br/comissoes/comissao?codcol=2504.

22. Vale ressaltar que, como o objetivo do artigo é trazer uma perspectiva mais específica a respeito dos pontos do Anteprojeto que podem vir a afetar o desenvolvimento conjunto de IoT e IA, não traremos descrição detalhada de todos os dispositivos do texto proposto pela CJSUBIA. Assim, aprofundaremos apenas alguns dos seus aspectos quando necessário para o contexto deste artigo e para a compreensão de como os dispositivos que se encontrem sob análise podem afetar o desenvolvimento e expansão de IoT relacionada à IA. Os artigos mais relevantes ao artigo serão mencionados e citados para quando se considerar oportuno.

trabalhados ao longo da proposta, que são definidos no art. 4º - o que pode dificultar sua própria concretização. Junto a isso, tem-se de considerar que o texto proposto pela CJSUBIA, inspirado nas discussões europeias, traz a perspectiva de regulação de IA pautada no risco relacionado ao sistema, tal como será visto abaixo, no item 3.2. Em breve síntese, sistemas diversos implicam em riscos diversos, que por sua vez implicam em obrigações distintas aos agentes. No entanto, a gradação de risco não é refletida expressamente quando se trata de direitos das pessoas afetadas, o que amplifica as dificuldades de concretização.

Parece excessivo – e mesmo contraditório com a lógica exposta no próprio texto – que os direitos garantidos sejam os mesmos para os casos de sistemas de IA de risco baixo, alto e excessivo. A partir de tal disposição, restaria criado ônus relevante para as empresas e desenvolvedores de sistemas de IA no país, mesmo quando seu uso é reconhecido pelo próprio Anteprojeto como baixo, o que poderia acabar desincentivando a inovação e o crescimento da indústria brasileira.

Há ainda um ponto relevante, especialmente no que diz respeito à interconexão entre IA e IoT, atinente à transparência que seria necessária para a concretização de tais direitos. Como já dito anteriormente, dispositivos que usam IoT não necessariamente são claros a esse respeito. Uma pessoa que utiliza uma assistente virtual ou um *smartwatch* não necessariamente compreende como funcionam tais dispositivos ou como eles se conectam a redes para troca e transferência de informações e dados, por vezes pessoais. Ou seja, não seria inesperado que, ao implementarem IA em dispositivos que usam IoT, existisse dificuldade por parte das empresas e dos desenvolvedores dessas tecnologias em informar as pessoas que os utilizam acerca da presença de IA e, consequentemente, sobre os possíveis direitos que teriam como "pessoas afetadas" por sistemas de IA. Essa questão pode parecer trivial, ao pensarmos que o esclarecimento seria muito simples, ou seja, bastaria informar ao usuário que ele tem direitos previstos numa determinada lei e indicar qual lei é essa. Mas esse tema se torna particularmente relevante ao constatarmos que, mesmo serviços e produtos que combinem IA e IoT via de regra não funcionam única e exclusivamente por meio de inteligência artificial. Há decisões que são tomadas recorrendo-se a essa tecnologia, e outras que não fazem uso dela. Esclarecer ao usuário essa diferença - e mesmo debater se os direitos das pessoas afetadas aplicar-se-ia a toda a relação do usuário com o dispositivo, ainda que o uso de IA seja pontual - tende a ser particularmente

desafiador.

Nesse aspecto, parece que o Anteprojeto tenta emular o estabelecimento de um sistema de direitos a determinadas pessoas (denominadas de pessoas afetadas por sistemas de IA) nos moldes do que a LGPD fez com os chamados "titulares de dados pessoais". Ainda assim, há uma diferença essencial aqui: enquanto a LGPD regulamenta o tratamento de dados pessoais, o Anteprojeto procura regular o desenvolvimento, uso e implementação de uma tecnologia como um todo (que, como já pontuado, é comumente referida como um conjunto de tecnologias e não como uma tecnologia unitária). O escopo de aplicação de direitos relacionados à IA, portanto, é substancialmente mais complexo.

Tratando de direitos especificamente previstos no Anteprojeto, as ditas pessoas afetadas por sistemas de IA teriam direito a: **(i)** receber, antes da contratação ou utilização do sistema de IA, informações claras e adequadas quanto ao caráter automatizado da interação e da decisão em processos ou produtos que afetem a pessoa, descrição geral do sistema, tipos de decisões, recomendações ou previsões que se destina a fazer e consequências de sua utilização para a pessoa, identificação de operadores do sistema de inteligência artificial, categorias dos dados pessoais utilizados, dentre outras;[23] **(ii)** solicitar explicação sobre a decisão, previsão ou recomendação do sistema de IA, com as informações a respeito dos critérios e procedimentos utilizados, assim como sobre os principais fatores que afetam previsão ou decisão específica;[24] **(iii)** contestar e solicitar revisão de decisões, recomendações ou previsões geradas por sistema de IA que produzam efeitos jurídicos relevantes ou que impactem de maneira significativa os seus interesses;[25] e **(iv)** a um tratamento justo e isonômico, sendo vedadas a implementação e uso de sistemas de IA que possam acarretar discriminação direta, indireta, ilegal ou abusiva.[26]

Há muitos aspectos aqui que poderiam ser discutidos no que diz respeito aos desafios que a implementação de tais previsões traz quando lidamos com dispositivos que combinam IA e IoT, mas focaremos aqui em alguns possíveis exemplos de uso

23. Ver o art. 7º do Anteprojeto.
24. Ver o art. 8º do Anteprojeto.
25. Ver o art. 9º, art. 10 e art. 11 do Anteprojeto.
26. Ver o art. 12 do Anteprojeto.

conjunto destas tecnologias que demonstram a complexidade de concretização de tais direitos. Voltemos então ao exemplo de *smartwatch* que coleta e faz a análise de dados para fins de avaliação da saúde do usuário, partindo da premissa de que há uso de sistema de IA (*machine learning*, por exemplo) nesse processo, em alguma medida. Ademais, para mostrar a complexidade dos direitos previstos no Anteprojeto, imaginemos que o *wearable* em questão seja comercializado pela empresa A, porém, o sistema de IA utilizado para a análise de dados com o objetivo de gerar *insights* sobre a saúde do usuário seja fornecido pela empresa B.

Nesse cenário, surgem diversas dúvidas quanto a como garantir os direitos desses usuários. A primeira questão e talvez a mais central seria se as pessoas que utilizam o *wearable* seriam "pessoas afetadas" por um sistema de IA, tendo em vista a ausência de descrição desse conceito no Anteprojeto, e, em caso positivo, em que medida essa afetação ocorreria. Considerando que sejam assim definidas para fins da aplicação do Anteprojeto, vale refletir sobre qual seria a maneira mais adequada de disponibilizar a informação de que, ao utilizarem o *smartwatch*, estarão sujeitas a sistema de IA, além de todas as outras informações exigidas nos termos do artigo 7º. Lembrando, novamente, que há uso de IA em algumas funcionalidades do produto, mas não em todas. Esse uso somente parcial da IA leva a um questionamento inclusive sobre se os direitos existiriam em relação a todas as funcionalidades do wearable, ou apenas e tão somente às funcionalidades específicas na qual a IA fosse aplicada - e, é claro, à evidente complexidade em esclarecer essas diferenças ao usuário e implementar os direitos em tal contexto.

Ademais, ainda de acordo com seu artigo 7º, o Anteprojeto afirma que as pessoas afetadas teriam o direito a saber quais são as categorias de dados pessoais utilizados para o funcionamento do sistema de IA. No entanto, como já tratado, no caso dos sistemas de IoT, pode-se coletar diversos dados não necessariamente vistos como pessoais (ex.: o *smartwatch* pode coletar qual seria o número de passos que uma pessoa dá em um dia) e, com base na IA, gerar novas informações que, em alguma medida, poderão ser consideradas pessoais (ex.: utilizar *machine learning* para determinar qual é a probabilidade de a pessoa ser sedentária ou não em razão do número médio de passos dados a cada semana). Não é claro como casos desse tipo seriam abordados, sendo que provavelmente a definição também dependerá de como o próprio conceito de dado pessoal será interpretado pela Autoridade Nacional de

Proteção de Dados ("ANPD") perante a LGPD.

Pensando em uma possível classificação do sistema de IA sobre se uma pessoa pode ser considerada sedentária com base nas informações coletadas por dispositivo de IoT, surge também o debate sobre a quem a pessoa deveria solicitar a revisão da decisão: **(i)** à empresa A, que comercializa o *smartwatch*; ou **(ii)** à empresa B, responsável pelo desenvolvimento do sistema de IA. Cabe igualmente indagar como solicitar a correção de dados que a pessoa considerar incorretos, se for o caso. De acordo com o Anteprojeto, a responsabilidade da correção, ao que tudo indica, seria dos agentes de IA, mas, no caso de dispositivo de IoT, os dados foram coletados pelo *smartwatch* e, por consequência, pela empresa que comercializa o *wearable*, e não pela empresa que efetivamente desenvolveu o sistema.

Ainda que o exemplo descrito seja relativamente simples, ele demonstra que há lacunas na aplicação dos direitos das "pessoas afetadas" por sistemas de IA que tendem a ser particularmente relevantes quando pensamos no uso conjunto de IA e IoT. Portanto, é provável que o texto do Anteprojeto, como se encontra atualmente, enfrente desafios particulares do ponto de vista de *enforcement*.

3.2. IMPACTOS DA CLASSIFICAÇÃO DE RISCO DO ANTEPROJETO

Como mencionado brevemente acima, o Anteprojeto propõe uma abordagem regulatória que leva em consideração os tipos de uso de sistemas de IA em relação aos riscos que eles acarretariam. Conforme o artigo 13 de seu texto, antes dos sistemas de IA serem disponibilizados no mercado ou antes de sua utilização, eles deveriam passar por uma avaliação preliminar sobre seu grau de risco, a ser realizada pelo fornecedor. O Anteprojeto, assim, separa os sistemas de IA em risco excessivo (cuja aplicação é vedada na maioria dos casos) e alto risco.

A premissa aqui adotada parece ser benéfica tanto para reguladores quanto para regulados. Se há riscos diversos representados pelos sistemas, também faz sentido que o ônus de cada desenvolvedor seja diferenciado. Em outras palavras, se o sistema em concreto representa maiores riscos, então deve haver maior cuidado (e consequentemente maiores requisitos) para seu uso e implementação. Isso permite que nem todos os sistemas sejam submetidos aos mesmos padrões de análise, evitando assim critérios muito rigorosos para aqueles que, em concreto, não apresentam

maiores preocupações, quanto permite uma avaliação de fato mais detalhada de sistemas que podem vir a significar algum padrão mais elevado de preocupação. A questão que parece menos clara, no entanto, é como exatamente essa classificação de risco foi feita, ou como será eventualmente atualizada. Em boa medida, essa premissa já se encontrava bem colocada na proposta europeia de regulação da IA e foi reproduzida aqui – inclusive no que diz respeito às categorias, que são muito semelhantes. Mas enquanto existe na União Europeia uma discussão um pouco mais bem colocada sobre revisão das categorias de risco e sobre a própria razão de ser da classificação, no caso brasileiro esse tema não fica tão claro.

Esse tema se torna particularmente relevante na medida em que se nota que, dentre as categorias de sistemas de IA de risco excessivo e alto risco, se encontram muitas áreas nas quais é comum o uso e a aplicação de IoT. Quando pensamos nas categorias colocadas como de alto risco por parte do Anteprojeto, alguns exemplos são: **(i)** uso para fins de dispositivos de segurança na gestão e funcionamento de infraestruturas críticas (ex.: sensores utilizados para coletar informações de trânsito)[27]; **(ii)** veículos autônomos; **(iii)** aplicações na área da saúde, inclusive destinadas a auxiliar em diagnósticos e procedimentos médicos; **(iv)** sistemas biométricos de identificação; e **(v)** na gestão da migração e controle de fronteiras (ex.: utilização de câmeras e sensores para identificar movimentos de possíveis imigrantes).[28] Portanto, os desenvolvedores de IoT cujos negócios sejam focados em tais áreas e que desejem realizar um uso conjunto de IA acabarão tendo de observar os termos do Anteprojeto, caso ele seja aprovado.

No caso dos sistemas de IA que são tidos como de risco excessivo, é notável a inclusão dos sistemas relacionados a atividades de segurança pública, sendo que o Anteprojeto permite somente a utilização dos sistemas de identificação biométrica à distância de maneira contínua em espaços acessíveis ao público, quando houver a previsão em lei federal específica e autorização judicial em conexão com a atividade de persecução penal individualizada nos casos de: **(i)** persecução dos crimes passíveis de pena máxima de reclusão superior a dois anos; **(ii)** busca de vítimas de crimes ou

27. O caso do próprio Cor, mencionado acima.

28. Os referidos exemplos são sistemas de IA de alto risco conforme o art. 17, I, VIII, IX, X e XIV do Anteprojeto.

pessoas desaparecidas; e **(iii)** crime em flagrante.[29] O uso de sistemas de IoT para a segurança pública é particularmente frequente quando pensamos nas *smart cities*.

Há muitas discussões a respeito das formas de vigilância que podem surgir[30]-[31] em razão da utilização de câmeras e de outros dispositivos (como sensores) e embates a respeito das consequências sociais de seu uso. É também natural e esperado que, na medida em que a tecnologia avance, esses debates levem à necessidade de atualização do panorama regulatório, inclusive para melhor proteger cidadãos.

Um exemplo prático do aumento da vigilância com uso de IoT é o Centro de Operações Rio ("Cor"), que fez parte do projeto Smarter Cities da IBM.[32] O Cor consiste em uma estrutura com salas de controle para fins de gerenciamento de atividades e também do dia a dia da cidade do Rio de Janeiro, monitorando desde o controle de tráfego até condições climáticas e mídias sociais.[33] Nesse contexto, o Cor poderia ser considerado um sistema avançado de controle e gerenciamento de cidades.[34] Além do Cor, existe, também na cidade do Rio de Janeiro, o chamado Centro Integrado de Comando e Controle ("Cicc"), o qual é dedicado exclusivamente a questões de segurança. Os centros de controle, tal como o Cicc, tiveram uma expansão durante a Copa do Mundo da Fifa de 2014, realizada no Brasil.

Tais centros foram criados nas doze cidades-sede da Copa, sendo o do Rio de Janeiro um polo de coordenação regional e o de Brasília o polo nacional.[35] Nessa conjuntura, há uma acentuação da vigilância entre os dois centros que se dá,

29. Ver o art. 15 do Anteprojeto.
30. FIRMINO, Rodrigo José. Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal. p. 69-70. In: BRUNO, F. et al (Orgs). Tecnopolíticas da vigilância. São Paulo: Editora Boitempo, 2018.
31. EVANGELISTA, Rafael de Almeida; SOARES, Tiago; SCHMIDT, Sarah; LAVIGNATTI, Felipe. DIO: O mapeamento coletivo de câmeras de vigilância como visibilização da informatização do espaço urbano. p. 396-397. In: BRUNO, F. et al (Orgs). Tecnopolíticas da vigilância. São Paulo: Editora Boitempo, 2018.
32. FIRMINO, R. J. Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal. In: BRUNO, F. et al (Orgs). Tecnopolíticas da vigilância. São Paulo: Editora Boitempo, 2018. p. 73.
33. Ibid., loc. cit.
34. Ibid., loc. cit.
35. Ibid., loc. cit.

essencialmente, por conta de um protocolo de entendimento que determina que o Cor (responsável pela gestão urbana), sempre que for requisitado, deverá compartilhar certas informações com o Cicc (responsável pela gestão da segurança).[36] Assim, esses centros de controle aparecem como a imagem mais forte e representativa de um certo tipo de gestão pautada na cidade inteligente centralizadora.[37]

Para o funcionamento do Cor e do Cicc, a utilização de IoT é praticamente uma exigência (é fatal que dados sejam tanto coletados quanto transmitidos por meio de sensores e câmeras, por exemplo). Assim, ao se pensar em sistemas de IA utilizados para identificação biométrica na segurança pública, como posto pelo Anteprojeto, há uma alta probabilidade de que se termine regulando o uso de IoT em tais contextos, especialmente porque a coleta dos dados a serem analisados por meio de IA devem decorrer da sua obtenção por câmeras de vigilância. Ao mesmo tempo, nota-se que esses sistemas de vigilância (potencialmente pautados por IA, inclusive) já são uma realidade no Brasil, tendo se aproveitado mesmo de uma ausência de regulação específica para se expandirem.[38]

O principal tema que vale observar num contexto como esse é que uma definição imprecisa de risco, ou falta de clareza sobre como análises de risco devem ser conduzidas, pode gerar classificações incorretas. Casos como o Cor e o Cicc parecem demonstrar que já existem aplicações hoje de sistemas de IA, utilizadas inclusive pelo Estado, que também fazem uso de IoT, que seriam classificados como de alto risco ou mesmo de risco excessivo. Parece improvável que estruturas como essas não se valham, em algum ponto, sistemas de IA. Ao mesmo tempo, é improvável que toda a estrutura do Cor e do Cicc seja pautada em tais sistemas. Assim, classificar os sistemas e aplicar o Anteprojeto a eles pode ser bem menos trivial se os considerarmos como um conjunto de aplicações. Um exemplo pode auxiliar a ilustrar essa questão. Se houver, no Cor, um sistema de IA que tenha sido desenvolvido inicialmente para rastreamento de veículos de modo a aplicar multas de trânsito e gerir o tráfego, isso

36. Ibid. p. 74.

37. Ibid. p. 74.

38. EVANGELISTA, Rafael de Almeida; SOARES, Tiago; SCHMIDT, Sarah; LAVIGNATTI, Felipe. DIO: O mapeamento coletivo de câmeras de vigilância como visibilização da informatização do espaço urbano. p. 396. In: BRUNO, F. et al (Orgs). Tecnopolíticas da vigilância. São Paulo: Editora Boitempo, 2018.

seria uma aplicação de IA no cerne de um conjunto de aplicações muito mais amplo, que talvez precise ser avaliado de maneira individualizada, mas que, se combinado com outros sistemas utilizados dentro da iniciativa mais ampla Cor/Cicc, pode revelar níveis de riscos distintos. Por conseguinte, surgem dúvidas sobre como tratar estruturas como o Cor e o Cicc e até mesmo a respeito de como seria o procedimento para identificar, nesses conjuntos de aplicações, obrigações e responsabilidades específicas relacionadas ao Anteprojeto.

Ademais, o Cor e o Cicc também ajudam a ilustrar uma outra complexidade, que chamaremos aqui de uso "off-label". Voltando ao hipotético rastreamento de veículos mencionado acima, caso esse sistema passe a ser empregado para finalidades que se desviam das originais – em concreto, se o sistema de IA passa a ser mobilizado para fins da persecução de crimes passíveis de pena máxima de reclusão superior a dois anos, como os que envolvem acidentes de trânsito, ele seria classificado como de risco excessivo nos termos do Anteprojeto. Se a finalidade é desviada, surge a questão: como fica a análise de risco? O desenvolvedor original do sistema terá feito um estudo pensando na utilização daquela ferramenta para uma finalidade específica, qual seja, o rastreamento de veículos. Mas se o uso envolver outra finalidade, caberia discutir se a responsabilidade recairia sob o próprio desenvolvedor – que deveria ter antecipado o potencial de uso de sua ferramenta para finalidade distinta da original – se apenas sob o operador – que afinal teve a ideia de uso off-label –ou se sobre ambos. Ainda, caberia questionar se seria necessário que o operador refizesse a avaliação de risco do sistema para esse novo uso, e mesmo se ele teria completas condições de fazer essa análise. Questões como essa não são respondidas de maneira peremptória pelo Anteprojeto, porém parece claro, a partir dos exemplos fornecidos, que é provável que elas surjam na aplicação práticas dos seus dispositivos legais, especialmente ao se levar em conta que o desenvolvimento tecnológico, frequentemente, ocorre de forma incremental e não linear, com sistemas complexos surgindo das combinações de sistemas mais simples.

Nesse contexto, como dito, se os sistemas de risco excessivo são exemplo de regulação que acaba por, muitas vezes, abranger o uso de IoT, as previsões do Anteprojeto que dizem respeito às obrigações que recaem sobre desenvolvedores e operadores de sistemas provavelmente aplicar-se-ão a muitas situações práticas em que haverá uma combinação de IA e IoT, e precisarão ser consideradas pelos agentes

envolvidos em tais processos.

3.3. DEFINIÇÃO DA AUTORIDADE REGULADORA

Conforme o artigo 4º, V, do Anteprojeto a autoridade competente para aplicação da legislação seria o órgão ou entidade da Administração Pública Federal responsável por implementar, fiscalizar e zelar pelo cumprimento do Anteprojeto em todo o território nacional. No entanto, apesar da definição, o Anteprojeto não traz em seu texto qual seria a autoridade em questão, limitando-se a dizer que caberá ao Poder Executivo defini-la, conforme o *caput* do seu artigo 32. Como esclarecido por membros da CJUSBIA, esse caminho foi trilhado na tentativa de evitar problemas que foram enfrentados quando da tramitação do projeto de lei que resultou na LGPD - em especial, o entendimento de que haveria vício de iniciativa de criação de nova autoridade se tal proposta não tivesse sido inserida no texto pelo próprio Poder Executivo. Evidente, no entanto, que a falta de definição precisa gera algum nível de insegurança jurídica, até mesmo no que diz respeito à aplicação das disposições legais, tendo em vista que cada tipo de regulador tende a adotar uma lógica específica à leitura dos dispositivos.

Nesse sentido, se a autoridade for uma já existente no quadro do Poder Executivo, o que parece particularmente provável dado o contexto fiscal atual, é possível que a regulação de IA termine enviesada para algum ramo específico do direito. Por exemplo, caso se escolha a ANPD, é possível que se dê maior relevância a aspectos da regulação que mais diretamente dialoguem com temáticas de proteção de dados pessoais e privacidade. Por outro lado, caso se escolha o Conselho Administrativo de Defesa Econômica, seria possível terminarmos com uma regulação mais focada em questões concorrenciais. Se autoridades setoriais fossem escolhidas, como a Agência Nacional de Telecomunicações ("Anatel") ou o Banco Central, a maior probabilidade seria de enfoque particular em segmentos de mercado já regulados por esses atores.

Refletindo especificamente sobre a Anatel como possível reguladora dos temas de IA, deve-se notar que o Decreto nº 9.854/2019 define IoT, em seu artigo 2º, I, como a infraestrutura que integra a prestação de serviços de valor adicionado ("SVA") com capacidades para conexão física ou virtual de coisas com dispositivos que se baseiam

em tecnologias da informação e comunicação existentes e nas suas evoluções com interoperabilidade. SVAs, por sua vez, são serviços regulados conforme artigo 61 da Lei nº 9.472/1997 (Lei Geral de Telecomunicações ou "LGT"). Assim, uma interpretação conjunta desses dispositivos legais poderia levar a entendimento segundo o qual a Anatel teria tendência a regular a IA a partir de um enfoque mais diretamente relacionado a IoT.

De toda forma, é certo que nenhuma das autoridades hoje existentes na estrutura do Executivo possui expertise no tema de IA. Por conseguinte, a escolha de qualquer uma delas, para ter sucesso, dependeria de esforço adicional de adaptação do regulador à temática. Ao analisarmos justamente a intersecção entre IoT e IA, surge uma preocupação adicional no sentido de que essas autoridades também não necessariamente conhecem o tema em profundidade ou, se o conhecem, tendem a conhecê-lo aplicado a um segmento específico (por exemplo, o uso de IoT na saúde ou no sistema financeiro ou o já mencionado caso de enquadramento de IoT como SVA) e não de forma global.

4. CONCLUSÕES

A partir do exposto, pode-se perceber que regulações sobre tecnologia, especialmente as que ainda são incipientes ou que estão em forte fase de expansão e de desenvolvimento, em certos casos, acarretam um risco de afetar outras tecnologias em razão de sua possível interconexão – e talvez no caso da inteligência artificial isso seja especialmente verdade, por conta de sua transversalidade, representando o caso IA e IoT apenas um exemplo dos muitos que surgirão. No caso demonstrado no artigo, o objetivo foi compreender, com base em reflexões iniciais, quais seriam os alguns dos possíveis impactos do Anteprojeto para fins do desenvolvimento de IoT. O que é possível concluir é que as interconexões tendem a ser amplas e algo abrangentes, demonstrando de forma ainda mais intensa a importância do amplo debate legislativo e das reflexões sobre o tema.

REFERÊNCIAS

ABSTARTUPS; BOX 1824; GOOGLE FOR STARTUPS. *O impacto e o futuro da Inteligência Artificial no Brasil*. 2022. Disponível em:

https://drive.google.com/file/d/1ETBrrCfpnaviNY3z8eQX3cXHNe7iq7uF/view.

COMISSÃO EUROPEIA. *What are smart cities*: Cities using technological solutions to improve the management and efficiency of the urban environment. Disponível em: https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law & Technology Review*, v. 18, 2017. Disponível em: https://scholarship.law.duke.edu/dltr/vol16/iss1/2/.

EVANGELISTA, Rafael de Almeida; SOARES, Tiago; SCHMIDT, Sarah; LAVIGNATTI, Felipe. DIO: O mapeamento coletivo de câmeras de vigilância como visibilização da informatização do espaço urbano. In: BRUNO, F. et al (Orgs.). *Tecnopolíticas da vigilância*. São Paulo: Editora Boitempo, 2018.

FIRMINO, Rodrigo José. Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal. In: BRUNO, F. et al (Orgs.). *Tecnopolíticas da vigilância*. São Paulo: Editora Boitempo, 2018.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OECD). The Internet of Things: Seizing the Benefits and Addressing the Challenges (Background report for Ministerial Panel 2.2). In: *Working Party on Communication Infrastructures and Services Policy*. Paris: OCDE, 2016. Disponível em: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En.

PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, 2014. Disponível em: https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf.

PETERS, Jay. Amazon is subjecting Alexa to a performance review: The Wall Street Journal reports that Alexa is one of the company's businesses under scrutiny as part of a cost-cutting review led by CEO Andy Jassy. *The Verge*, 2022. Disponível em: https://www.theverge.com/2022/11/10/23451534/amazon-alexa-cost-cutting-review-andy-jassy.

PODESTA, Arianna; TSONI, Maria. Commission clears acquisition of Fitbit by Google, subject to conditions. *Comissão Europeia*, 2020. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

SATARIANO, Adam; WAKABAYASHI, Daisuke. Google to Buy Fitbit for $2.1 Billion: The deal represents an aggressive attempt by Google to bolster its lineup of hardware products. *The New York Times*, 2019. Disponível em: https://www.nytimes.com/2019/11/01/technology/google-fitbit.html.

SCHATSKY, David, KUMAR, Navya, BUMB, Sourabh. Bringing the Power of AI to the Internet of Things. *The Wired*. Disponível em: https://www.wired.com/brandlab/2018/05/bringing-power-ai-internet-things/.

US COMMERCIAL SERVICE. *Top Global Artificial Intelligence Markets Report*. Department of Commerce of the United States of America, 2021. Disponível em: https://www.trade.gov/sites/default/files/2022-05/Top%20Global%20AI%20Markets%20Report%204.20%20%282%29%20%281%29.pdf.

YOO, Christopher S. The Emerging Internet of Things Opportunities and Challenges for Privacy and Security. In: *Governing Cyberspace during a Crisis in Trust*. Centre for International Governance, 2019. Disponível em: https://www.cigionline.org/articles/emerging-internet-things/.

II
RESPONSABILIDADE CIVIL, ATUAÇÃO PROFISSIONAL E ILÍCITOS CIVIS

INTERNET DAS COISAS E O SEMPRE NOVO TEMA DA RESPONSABILIDADE: ALGUMAS REFLEXÕES

Marcelo de Oliveira Milagres
Professor Associado na Faculdade de Direito da UFMG.

DOI: https://doi.org/10.59224/dti5.ch3

Resumo: A internet das coisas é uma realidade. A conectividade de diversos dispositivos, para fins variados, enseja discussões técnicas, econômicas e jurídicas. O artigo traz algumas reflexões sobre o tema sempre novo da responsabilidade civil, com ênfase no fomento dos avanços da ciência.
Palavras-chave: IoT; Responsabilidade; Tecnologia; Regulação.

Abstract: *The internet of things is a reality. The connectivity of different devices, for different purposes, gives rise to technical, economic and legal discussions. The article presents some reflections on the ever-new subject of civil liability, with an emphasis on promoting advances in science.*
Keywords: *IoT; Liability; Technology; Regulation.*

1. CONSIDERAÇÕES INICIAIS

É sempre com muita alegria e elevada apreensão que recebo o generoso convite dos professores organizadores para participar deste consagrado projeto de "Direito, Tecnologia e Inovação".

Alegria – pela rica e inestimável oportunidade de compartilhar esse valioso espaço com renomados pesquisadores; apreensão – pela reconhecida ausência de

conhecimento de uma área tão incrivelmente dinâmica e desafiante.

Fiquei pensando sobre alguma contribuição de um professor de Direito Civil, particularmente de Direito das Coisas, sobre um tema tão complexo que é a internet das coisas (IoT).

Em verdade, aos contemporâneos desafios da vida é possível acrescentar, com os ajustes necessários, alguns clássicos instrumentos do direito privado. Não é desconhecida, pois, a discussão sobre usucapião de bens incorpóreos, acerca da qual há que se lembrar dos trabalhos dos professores Luciano de Camargo Penteado[1], Judith Martins-Costa[2], Pedro Marcos Nunes Barbosa[3] e Cássio Augusto Barros Brant[4].

Luciano de Camargo Penteado, ao trazer a lição dos romanos, *usucapio autem quae est corporalium rerum concessa,* defende que se pode "possuir uma coisa, submetendo-a ao domínio da vontade, como quando se ocupa – possuindo – um apartamento. Já as ideias não se ocupam. Podem ser empregadas, mas empregar a ideia alheia, de boa-fé, é muito diferente de as possuir como dono"[5].

Por sua vez, Judith Martins-Costa defende a possibilidade de usucapião de bens incorpóreos. "Aceita, no plano teórico-dogmático, a *possessio iuris;* realizada, no plano positivo, a extensão conceitual da propriedade e da posse aos bens imateriais; e confirmada, no plano prático, a documentabilidade de *res incorpórea,* que segue, no direito societário, formas e registros próprios, nada há a impedir a aquisição da propriedade (titularidade) por usucapião àqueles que, no prazo legalmente cominado à usucapião de coisas móveis, detém a posse (legitimidade) dessas ações [ações

1. PENTEADO, Luciano de Camargo. Que coisa é a coisa? Reflexões em torno a um pequeno ensaio de Carnelutti. *Revista de direito privado,* São Paulo, n. 39, jul./set. 2009, p. 249-258.
2. MARTINS-COSTA, Judith. Usucapião de coisa incorpórea: breves notas sobre um velho tema sempre novo. In.: TEPEDINO, Gustavo; FACHIN, Luiz Edson (Coords). *O direito e o tempo:* embates jurídicos e utopias contemporâneas: estudos em homenagem ao Professor Ricardo Pereira Lira. Rio de Janeiro: Renovar, 2008, p. 631-653.
3. BARBOSA, Pedro Marcos Nunes. *Direito civil da propriedade intelectual:* o caso da usucapião de patentes. 3. ed. Rio de Janeiro: Lumen Juris, 2016.
4. BRANT, Cássio Augusto Barros. *Usucapião na propriedade intelectual.* Belo Horizonte: D'Plácido, 2014.
5. PENTEADO, Luciano de Camargo. Que coisa é a coisa? Reflexões em torno a um pequeno ensaio de Carnelutti. *Revista de direito privado,* São Paulo, n. 39, jul./set. 2009, p. 256.

ao portador, nominativas e escriturais]".[6]

Pedro Marcos Nunes Barbosa entende "a posse de direitos, ou uma posse qualificada nos bens imateriais, forte a provocar a ampliação ou transferência de titularidades"[7] e apresenta a tese da *usucapião inclusiva:* "[...] a usucapião no seu âmbito *normal* implicaria na simultânea constituição de um direito real, com a perda (pelo menos da exclusividade ou total abrangência) de algum atributo que antes concentrava. Contudo, a natureza *ubíqua* da propriedade imaterial permitirá uma *usucapião inclusiva* [...]".[8]

Para Cássio Augusto Barros Brant, a "usucapião na propriedade intelectual tem como objetivo dar destinação às obras ou inventos que foram abandonados por seus detentores do direito de uso, colocando em prática o dever social e econômico que esse tipo de propriedade possui"[9].

Recentemente, refletindo sobre o possível fundamento do valor cobrado pelo cancelamento de uma viagem pelos aplicativos de transporte (taxa de cancelamento), concluí que este se deve a um provável mecanismo contratual de execução privada e, também, ao antigo instrumento das arras penitenciais.

Como se vê, as consequências do emprego da tecnologia do nosso tempo podem ser avaliadas a partir de instrumentos jurídicos de ontem, mas, reitere-se, com o olhar da contemporaneidade, da denominada Quarta Revolução Industrial.

Dessarte, quanto à internet das coisas, em uma primeira e não refletida abordagem, haveria um importante ponto de contato entre as realidades antiga (coisa) e a contemporânea (internet), vale dizer, o próprio objeto, ou seja, a coisa.

À evidência e em uma perspectiva mais restrita – não menos técnica –, pode-se

6. MARTINS-COSTA, Judith. Usucapião de coisa incorpórea: breves notas sobre um velho tema sempre novo. In.: TEPEDINO, Gustavo; FACHIN, Luiz Edson (Coords). *O direito e o tempo:* embates jurídicos e utopias contemporâneas: estudos em homenagem ao Professor Ricardo Pereira Lira. Rio de Janeiro: Renovar, 2008, p. 653.
7. BARBOSA, Pedro Marcos Nunes. *Direito civil da propriedade intelectual:* o caso da usucapião de patentes. 3. ed. Rio de Janeiro: Lumen Juris, 2016, p. 87.
8. Op. Cit., p. 12.
9. BRANT, Cássio Augusto Barros. *Usucapião na propriedade intelectual.* Belo Horizonte: D'Plácido, 2014, p. 168.

atribuir à coisa a natureza corpórea em contraposição aos bens que alcançariam realidades materiais e imateriais, corpóreas ou incorpóreas[10]. Parece, contudo, que o maior enfoque na matéria não está no aspecto material ou externo, e, sim, na inteligência e na inventividade que possibilitam conexões cada vez mais avançadas entre aparelhos, objetos e instrumentos que circundam a nossa vida.

Venho afirmando, a partir de um olhar da nossa realidade, que dois mundos coexistem: o corpóreo e o incorpóreo. Não se pode, por exemplo, prescindir da matéria veículo; igualmente, todos são dependentes da tecnologia que inserida na vida.

Na perspectiva do jurista, toda relação é intersubjetiva. Nesse diapasão, todas as coisas são objeto das nossas interações.

Como defender, pois, interações entre as mais diversas coisas a partir da rede mundial de computadores?

No plano da tecnologia, não se desconhece a conectividade entre máquinas, instrumentos, objetos e diversos suportes físicos.

Quais os olhares do jurista para essa realidade?

Inicialmente, e já escrevi sobre a temática[11], em que pese o avanço da denominada inteligência artificial, não há uma personificação das coisas; as relações jurídicas permanecem intersubjetivas. As coisas se inserem como objeto dessas relações.

A conectividade das coisas não lhes atribui a qualidade de pessoas tampouco a de sujeitos de direito, embora, no plano jurídico, deve-se reconhecer que a noção de subjetividade é mais ampla do que a de personalidade. Nem todos os titulares de

10. Segundo Paulo Victor Reis, "Bens são coisas materiais ou imateriais que possuem valor econômico, ou certo aspecto de raridade ou atributo esgotável, que podem servir de objeto em uma relação jurídica, enquanto que coisa é matéria útil à satisfação das necessidades do homem, quer sejam esgotáveis ou passí-veis de apropriação. Portanto, coisa é tudo aquilo que existe na natureza, seja valioso ou não, disponível ou não e com conteúdo ou valor econômico ou não, que para o ser humano torna-se passível de apropriação figurando como objeto de uma relação jurídica. Contudo, existem coisas que não são suscetíveis de apropriação, a exemplo o ar ou a luz solar. Mas todos os bens jurídicos são coisas, enquanto apenas algumas coisas são bens jurídicos." (REIS, Paulo Victor Alfeo. *Algoritimos e o direito.* São Paulo: Almedina, 2020, p.157)

11. MILAGRES, Marcelo de Oliveira. A robótica e as discussões sobre a personalidade eletrônica. In.: EHRHARDT JR., Marcos; CATALAN, Marcos; MALHEIROS, Pablo (Org.). *Direito civil e tecnologia*. Belo Horizonte: Fórum, 2020, p. 509-518.

direitos e de obrigações são dotados de personificação (sociedade não personificada, sociedade irregular, massa falida, espólio, herança jacente e vacante, condomínio edilício).

Apesar disso, Gunther Teubner defende que o direito privado tem uma escolha: reconhecer a responsabilidade às máquinas autônomas ou admitir um número crescente de acidentes sem responsáveis. Segundo o autor, quando os robôs tomam decisões independentes, há que se lhes reconhecer *personalidade eletrônica*[12].

O debate é intenso.

Segundo Silvia Díaz Alabart, "la ersonalidade jurídica específica para los robots, que podemos denominar personalidade electrónica, o debería ser otra cosa que una capacidade jurídica bastante limitada en razón a su objetivo indemnizatorio ya señalado. No se trataría de hacer a los robots inteligentes sujetos de derechos de forma general, sino que con esa personalizazición limitada se eliminarían algunos problemas para que se pueda hacer efectiva la indemnización por los daños causados"[13].

Um dos grandes pontos dessa temática da internet das coisas parece ser o sempre antigo e novo tema da responsabilidade civil – antigo, porquanto os prejuízos fazem parte da realidade da vida; novo, porque, embora reconhecido o instituto, as suas roupagens devem ajustar-se à contemporaneidade, não de um *modismo,* de um momento, mas de uma realidade dinâmica.

Sem o propósito de estabelecer limites ou certezas, algumas reflexões são necessárias: a) haveria a possibilidade de um regime único de responsabilidade pelos danos decorrentes da internet das coisas? b) em razão da diversidade da titularidade de objetos, que se conectam ou interagem por uma mesma plataforma ou um mesmo sistema, a indagação sobre o nexo de causalidade na definição da responsabilidade civil ainda seria pertinente?

12. TEUBNER, Gunther. *Digital personhood?* The status of autonomous software agentes in private law. Tradução de Jacob Watson. Société Suisse des Juristes: Ancilla Iuris, 2018, p. 113: "When robots make autonomous decisions, they should be recognized as "electronic persons", as legal entities in the full sense of the word".

13. ALABART, Silvia Díaz. *Robots y responsabilidade civil.* Madrid: Reus editorial, 2018, p. 77.

2. RESPONSABILIDADE CIVIL: REVISITANDO OS SEUS PRESSUPOSTOS

O tema da responsabilidade civil é rico de abordagens doutrinárias e, no aspecto prático, são diversos os julgados sobre a matéria.

Como bem aponta Caio Mário da Silva Pereira, é antiga a abordagem da responsabilidade civil: "[...] nos mais antigos monumentos legislativos, que antecederam por centenas de anos a civilização mediterrânea, vestígios há de que o tema fora objeto de cogitações. Vem do ordenamento mesopotâmico, como do Código de Hamurabi, a ideia de punir o dano, instituído contra o causador um sofrimento igual; não destoa o Código de Manu, nem difere essencialmente o antigo direito Hebreu."[14]

Segundo Carlos Roberto Gonçalves, o "surto do progresso, o desenvolvimento industrial e a multiplicação dos danos acabaram por ocasionar o surgimento de novas teorias, tendentes a propiciar maior proteção às vítimas"[15].

José Jairo Gomes destaca que a "novel ordem social trouxe consigo novos problemas que nem o jurista, nem o legislador podiam ignorar, urgindo buscar novas soluções. Impunha-se o arejamento da doutrina da culpa como fundamento da responsabilidade civil, a fim de torná-la mais flexível e adaptável aos reclamos da sociedade industrial e consumista. E mais: impunha-se o desenvolvimento de uma nova teoria para fundamentar a responsabilidade"[16].

Então, o que há de novo?

Os desafios são dinâmicos. A realidade advinda tecnologia traz o desafio de pensar diferentes soluções para os problemas do nosso tempo. Talvez se possa falar em novos ou diferentes danos.

Como acentua Paulo Victor, "o uso dos algoritmos implica em novos desafios que, até o presente momento, não eram objeto de discussão ou preocupação do Direito, logo, os institutos jurídicos até então existentes podem não ser mais úteis ou aplicáveis, tornando necessário o desenvolvimento de novos raciocínios e soluções jurídicas para sua proeminência. Diante de tal realidade, é necessário adaptação e

14. PEREIRA, Caio Mário da Silva. *Responsabilidade civil.* 8. ed. Rio de Janeiro: Forense, 1996, p. 1.
15. GONÇALVES, Carlos Roberto. *Responsabilidade civil.* 11. ed. São Paulo: Saraiva, 2009, p.6.
16. GOMES, José Jairo. *Responsabilidade e eticidade.* Belo Horizonte: Del Rey, 2005, p. 230.

abertura por parte dos juristas a essas relações algorítmicas, ou a inter-relações e intermediações por algoritmos em inúmeras áreas da vida, no sentido de se repensar a configuração de suas profissões ou de se reconciliar com as tecnologias. A não adaptação do profissional em tempos disruptivos pode implicar diretamente na não-sobrevivência do profissional no mercado de trabalho"[17].

Talvez, um dos grandes pontos de destaque, em razão do avanço da tecnologia, seja a preocupação com a proteção de **dados pessoais**. Nesse sentido, são importantes as iniciativas legislativas do Marco Civil da Internet (Lei n.º 12.965/2014) e da Lei Geral de Proteção de Dados – LGPD (Lei n.º 13.709/2018). Termos, até então, distantes passaram a fazer parte das conversas: *fake profile, hate speech, cyberstalking, data leak, chatbot.*

O uso indevido da tecnologia, inclusive por meio das redes sociais, pode ensejar a discussão de uma autoria não definida de prejuízos, de uma realidade de banalização, com difícil – talvez, impossível – identificação de autoria. Estar-se-ia diante de ilícitos sem rosto ou de danos anônimos?

Com o reconhecimento da responsabilidade objetiva, é aceita a tese do ilícito sem culpa. Hoje, pode-se pensar em ilícitos sem rosto ou sem autoria identificada, o que, em razão da própria necessidade de satisfação dos prejuízos suportados pelas vítimas, não afasta a necessidade de mecanismos de imputação.

Para Claudio Luiz Bueno de Godoy, a teoria do risco integral é revelação da causalidade pura. "Ou seja, a causalidade substitui a culpa sem nenhum elemento qualificador que a ela se agregue. A configuração do dever reparatório surge do só nexo que há entre o dano e um fato humano, até mesmo independente da vontade ou da consciência do agente. Basta apenas que a conduta humana seja a causa material da eclosão do evento lesivo, como que se a questão indenizatória daí decorrente se resolvesse à luz de um conflito de patrimônios, dessarte a que estranha qualquer cogitação de dado outro da ocorrência ou do causador do dano."[18]

A criação, a produção, a comercialização e o uso de máquinas autônomas, por si sós, seriam fundamento para a responsabilização de todos (pessoas naturais e

17. REIS, Paulo Victor Alfeo. *Algoritimos e o direito.* São Paulo: Almedina, 2020, p.147.
18. GODOY, Cláudio Luiz Bueno de. *Responsabilidade civil pelo risco da atividade.* São Paulo: Saraiva, 2009, p.65.

jurídicas) que se inserem nessa dinâmica relação jurídica? Seria preciso avaliar, no caso concreto, o nexo de causalidade?

Nessa perspectiva objetiva de responsabilização, não se afigura razoável o risco do desenvolvimento como excludente de responsabilidade. Razão parece assistir a Sergio Cavalieri Filho, para quem "os riscos de desenvolvimento devem ser enquadrados como *fortuito interno* – risco integrante da atividade do fornecedor, pelo que não exonerativo da sua responsabilidade"[19].

Não se pode impedir o necessário e o desejado avanço da técnica, mas não se pode, igualmente, deixar sem respostas eventuais resultados prejudiciais pelo alto risco das tecnologias emergentes. Nessa perspectiva, talvez se possa defender a regra da responsabilidade objetiva pela causalidade pura. A Resolução do Parlamento Europeu de 16 de fevereiro de 2017, no item 54, reconhece essa possibilidade: "Observa, ao mesmo tempo, que a responsabilidade objetiva exige apenas a prova de que o dano ocorreu e o estabelecimento de um nexo de causalidade entre o funcionamento prejudicial do robô e os danos sofridos pela parte lesada."

Ainda que se defenda responsabilidade civil sem ilícito[20], sem culpa e sem nexo de causalidade, não se pode afirmar responsabilidade sem dano[21].

É preciso reconhecer o prejuízo para se atribuir uma resposta indenizatória (com as discussões sobre as suas funções: reparatória, compensatória e/ou punitiva) em favor do ofendido e mediante alguma forma de imputação, seja contratual ou extracontratual.

Em razão dos desafios trazidos pela Iot, haveria a possibilidade de um regime jurídico único de responsabilidade civil?

19. CAVALIERI FILHO, Sergio. *Programa de responsabilidade civil.* 11. ed. São Paulo: Atlas, 2014, p. 233.
20. USTÁRROZ, Daniel. *Responsabilidade civil por ato lícito.* São Paulo: Atlas, 2014.
21. Cf. CARRÁ, Bruno Leonardo Câmara. *Responsabilidade civil sem dano:* uma análise crítica. Limites epistêmicos a uma responsabilidade civil preventiva ou por simples conduta. São Paulo: Atlas, 2015.

3. A (IM)POSSIBILIDADE DE UM REGIME JURÍDICO ÚNICO DE RESPONSABILIDADE PELOS DANOS NO ÂMBITO DA INTERNET DAS COISAS

A conexão de dispositivos e aparelhos à internet e a conexão entre eles parece alcançar um universo crescente: geladeiras inteligentes, lâmpadas *smart*, carros autônomos, *smartwatches*, *smart homes*, *smart cities*, drones e equipamentos médicos.

Não se pode desconsiderar a dinamicidade da indústria na projeção e na confecção de sensores e de dispositivos cada vez mais avançados.

Daí, uma provocação: seria possível um regime jurídico único de responsabilidade pelos danos no âmbito da internet das coisas?

Segundo Eduardo Bittar, o "tratamento conferido à responsabilidade por danos em ambiente virtual vem alcançando, para além das regras gerais da responsabilidade, uma enorme complexidade, devendo-se identificar e colher as específicas nuances, a partir dos diplomas legais incidentes sobre o caso concreto"[22].

Discutem-se, por exemplo, as nuances da responsabilidade civil envolvendo a Iot no âmbito das questões de saúde[23].

Não se desconhecem, outrossim, notícias envolvendo acidentes de veículos autônomos. Aos 24 de novembro de 2022, em São Francisco, na Califórnia, Estados Unidos da América, ocorreu um acidente com o veículo marca-modelo Tesla Model S, que, segundo consta, teve como causa falha do piloto automático[24]. Também, aos 5 de novembro de 2022, na província chinesa de Guangdong, um veículo da Tesla, Modelo Y, por causa não identificada, vitimou duas pessoas[25].

22. BITTAR, Eduardo C. B. O direito na era digital: responsabilidade civil e penal pelo uso indevido das redes sociais. In.: SARLET, Ingo Wolfgang; SARLET, Gabrielle B. Sales; BITTAR, Eduardo C.B. *Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital.* São Paulo: Expressa Jur, 2022, p. 17.
23. GENNARI, Francesca. What liability with the internet of things? Insights from the european case-law of the pip affair. Journaul Global jurist. https://doi.org/10.1515/gj-2022-0032.
24. Disponível em: <https://mundoconectado.com.br/noticias/v/30811/carro-da-tesla-para-sozinho-e-causa-engavetamento-de-8-veiculos-na-california-veja-video>. Acesso em: 14 mar. 2023.
25. Disponível em: <https://www.tecmundo.com.br/mobilidade-urbana-smart-cities/254317-acidente-tesla-deixa-duas-pessoas-mortas-china.htm>. Acesso em: 14 mar. 2023.

A resposta parece intuitiva. Não há a possibilidade de um regime jurídico único de direito dos danos provenientes da IoT. Não se pode desconsiderar a natureza das relações, se contratual ou extracontratual. Igualmente, a finalidade preponderante dos dispositivos: saúde, consumo, indústria, recreação, segurança.

A tecnologia emergente, por si só, não afasta todo o histórico de estudos e iniciativas legislativas sobre responsabilidade por conduta ou fato de terceiro, por eventos no âmbito das relações de consumo, médicas, enfim, toda uma sorte de situações da vida.

No plano nacional, subsiste todo um sistema normativo geral trazido pelo Código Civil, com destaque para as categorias de ilícito (arts. 186 e 187) e um capítulo sobre a resposta ou a responsabilidade (arts. 927 a 954), o que não afasta, por óbvio, um possível diálogo entre as formas de resposta (arts. 200 e 935 do Código Civil e 315 do Código de Processo Civil) e com os sistemas específicos de regulação: responsabilidade das pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos (art. 37, § 6º, da Constituição da República); responsabilidade civil por danos nucleares (art. 21, XXIII, *d,* da Constituição da República); reponsabilidade por práticas anticoncorrenciais (Lei n.º 12.529/2011**);** responsabilidade objetiva por risco integral (Lei n.º 10.744/2003), responsabilidade no âmbito das relações de consumo (Lei n.º 8.078/1990), entre outras situações.

Constatado o dano, é preciso verificar a natureza, a funcionalidade e o propósito dos dispositivos de IoT, bem como o sistema em que estão conectados, para construir uma melhor resposta para a reparação/compensação/punição decorrente do evento lesivo.

Como já se destacou a propósito do veículo autônomo: "[...] diante de uma possibilidade de acidente de trânsito, deverá primar pela vida do transeunte, ou pela vida do proprietário do veículo? Quem será o responsável por ditar a equação pela qual o algoritmo será regido? Essas respostas ainda não estão claras no desenvolvimento destes veículos do futuro, mas em algum momento precisarão estar. Quem serão os responsáveis por esses acidentes e cálculos matemáticos, os engenheiros? O desenvolvedor? A empresa? O proprietário do veículo? E pelos acidentes por meros erros

de sistema?"[26]

Se o próprio dispositivo de IoT apresenta falha de projeção, confecção e funcionamento, não se pode desconsiderar a responsabilidade do projetista, do construtor, enfim, daquele que idealizou e construiu o equipamento. Se o equipamento se insere em relação de consumo, aplica-se regime jurídico próprio, com o destaque para a reconhecida vulnerabilidade do consumidor e toda a dinâmica da produção probatória.

Ausente essa relação de consumo e diante do risco-criado pelos equipamentos, pode-se defender a responsabilidade de natureza objetiva e a possibilidade da distribuição judicial do ônus da prova.

Segundo o § 1º do art. 373 do Código de Processo Civil, "nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído".

No âmbito da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei n.º 13.709/2018), reconhece-se a possibilidade de inversão do ônus da prova: "o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa."

As questões – tanto de ordem material quanto procedimental – são várias. Diante da dificuldade de um regime jurídico único, poder-se-ia defender uma autorregulação de natureza setorial. Todavia, Silvia Díaz Alabart adverte que "sin minusvalorar la conveniencia de la existência de dichos códigos de conducta, la realidad de las cosas há demostrado que la autorregulación de cualquier sector industrial o comercial es insuficiente para garantizar la protección del consumidor. Es precisa una

26. SIQUEIRA NETO, José Francisco; MIRANDA, Lorrayne Barbosa; LANNES, Yuri Nathan da Costa. Inteligência artificial e veículos autônomos: aspectos éticos, políticos e jurídicos. In.: FABRI, Andréa Queiroz; Nascimento, Carlos Eduardo do; PINTO, Felipe Chiarello de Souza (coords). *Compliance and technology law*. Uberlândia: Composer, 2020, p. 237.

regulación adecuada que tome en cuenta el interés del consumidor (primordial en cuanto a su integridad física), además del interés de la investigación y de los comerciantes"[27].

No âmbito interno, destaca-se o Decreto n.º 9.854, de 25 de junho de 2019, que institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas.

Segundo o art. 2º, I, do referido Diploma, IoT é a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade.

Destaquem-se os objetivos do Plano Nacional de Internet das Coisas (art. 3º): (i) - melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT; (ii) - promover a capacitação profissional relacionada ao desenvolvimento de aplicações de IoT e a geração de empregos na economia digital; (iii) incrementar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT, por meio da promoção de um ecossistema de inovação neste setor; (iv) buscar parcerias com os setores público e privado para a implementação da IoT; (v) aumentar a integração do País no cenário internacional, por meio da participação em fóruns de padronização, da cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de IoT desenvolvidas no País.

Nessa regulação da IoT, busca-se priorizar sua aplicação aos ambientes de saúde, cidades, indústrias e rural (art. 4º), com observância dos seguintes temas (art. 5º): (i) ciência, tecnologia e inovação; (ii) inserção internacional; (iii) educação e capacitação profissional; (iv) infraestrutura de conectividade e interoperabilidade; (v) regulação, segurança e privacidade; (vi) viabilidade econômica.

No âmbito da regulação e da implementação do Plano Nacional de IoT, destaca-se a participação do Ministério da Ciência e Tecnologia e da Agência Nacional de Telecomunicações (Anatel).

27. ALABART, Silvia Díaz. *Robots y responsabilidade civil.* Madrid: Reus editorial, 2018, p. 29.

Com efeito, realizando-se comunicação entre dispositivos por redes de telecomunicações, não há dúvida da importância da regulação pela Anatel. Nesse sentido, destaca-se o Regulamento de Serviços e Telecomunicações, aprovado pela Resolução n.º 73/1998. A melhor conectividade dos dispositivos, por óbvio, pressupõe redes eficientes. Nesse diapasão, destacam-se as tecnologias denominadas Low Power Wide Area Network (LPWAN), NB-IoT (Narrowband IoT), SigFox e Long Range (LoRa).

Pode-se inserir um outro elemento para o debate. Em algumas situações, no âmbito da IoT, subsiste uma interação entre objetos/dispositivos de titularidade distinta. Constatado o prejuízo, qual seria a forma de imputação e a sua extensão?

4. A INTERAÇÃO ENTRE OBJETOS DE TITULARIDADE DISTINTA E OS PREJUÍZOS PROVOCADOS: QUEM PODE E QUEM DEVE INDENIZAR?

É conhecida a teoria geral sobre os fatos jurídicos em sentido amplo, que compreende fato jurídico em sentido estrito, ato, negócio e ato-fato jurídico.

As ações de dispositivos e equipamentos eletrônicos que se conectam e se interagem de diversas e múltiplas formas podem significar resultados danosos, não, necessariamente, um *ato digital ilícito.* O foco parece ser no prejuízo experimentado pelo usuário da IoT, e não mais na natureza ou na conduta, se há – ou não – uma ilicitude no denominado ato digital. Nesse diapasão e a despeito de uma política legislativa que afaste a discussão sobre o nexo de causalidade, a realidade pode trazer várias hipóteses ou condições que contribuem para os prejuízos: defeitos ou manuseio incorreto dos dispositivos, erros na programação, falta de informação, acesso indevido dos sistemas, falhas nas redes de comunicação.

Segundo Silvia Díaz Alabart, ao discutir a responsabilidade civil no âmbito da robótica, os danos "pueden proceder de algún defecto en la fabricación o programación de los robots, de falta de información sobre su funcionamento o información incorrecta de, inadecuación del tipo de robot a las tareas que se le han assignado, o incluso del uso incorrecto de los mismos por el usuario"[28].

Primeiramente, é preciso assegurar que os sistemas ou programas que possibilitam a comunicação entre os dispositivos sejam suscetíveis de auditoria, sejam

28. ALABART, Silvia Díaz. *Robots y responsabilidade civil.* Madrid: Reus editorial, 2018, p. 61.

transparentes.

É manifesta a dificuldade trazida pela *black box*, ou seja, a opacidade algorítmica, os desenhos ou programas de inteligência artificial que não permitem a adequada fiscalização, o necessário controle. Essa ausência de transparência não pode significar irresponsabilidade, mas a própria imputação de eventuais prejuízos aos programadores, àqueles que desenharam o programa ou o sistema obscuro. Para André Ramos Tavares[29], "a questão central da sindicabilidade ou explicabilidade algorítmica é um pressuposto que, se não for alcançável ou viável tecnologicamente, sequer demandará uma análise no plano da falta de responsabilidade para fins de estabelecermos (juridicamente) certos bloqueios de seu uso".

De outro lado, esses programas devem ser seguros, afastando o risco de acesso indevido por terceiro (*hacker*) que, inadvertidamente, pode desorganizar o funcionamento da IoT. Esse risco não afastaria a responsabilidade do programador ou do próprio titular do dispositivo da IoT. Nessa hipótese de intervenção de terceiro, pode-se afirmar a figura do fortuito interno.

Segundo a doutrina, esse fortuito "se relaciona com a pessoa do devedor ou da empresa e com a organização que eles imprimam ao negócio. Em contrapartida, o fortuito externo, também conhecido como força maior, é um fato que não guarda conexão com essas pessoas, tratando-se de um acontecimento externo a elas"[30]. O risco de acesso indevido ao sistema de IoT é uma realidade; não se trata de um evento externo à atividade.

Não se pode, outrossim, afastar eventual responsabilidade pelo fato do produto em razão de defeitos das *coisas*, dos próprios dispositivos materiais.

Segundo Jesús Jimeno Muñoz, de "tal forma, parece que se extiende el régimen de responsabilidade de los fabricantes y provedores de los productos que forman parte del IoT a la mayor parte de los efectos del funcionamento del produto, ya que el IoT sustituye la actuación del usuario por la interacción automática y programada. Así, la máxima de que el produto es defecutoso sí no oferece la seguridade que

29. TAVARES, André Ramos. *O juiz digital:* da atuação em rede à justiça algorítmica. São Paulo: Expressa, 2022, p. 24.

30. BRAGA NETTO, Felipe; ROSENVALD, Nelson; FARIAS, Cristiano Chaves. *Novo tratado de responsabilidade civil.* 2. ed. São Paulo: SaraivaJur, 2017, p. 483-484.

legitimamente cabría esperar se extiende al funcionamento autónomo del mismo"[31].

No âmbito da IoT, é preciso segurança dos dispositivos, da rede e do sistema.

Diante de possível dificuldade na identificação do autor do dano ou mesmo da constatada dificuldade econômica desse autor, pode-se estabelecer uma política de seguro obrigatório pelo implemento da Iot que cause maiores impactos. Para Silvia Díaz Alabart, uma consequência "de la aseguración obligatoria de cualquier actividad es el aumento de las reclamaciones por daños causados, producido por las mayores probabilidades de ser indemnizado, independentemente de la solvência patrimonial del causante material del daño"[32].

Nesse ponto e à guisa de uma necessária análise econômica, objeto de outras reflexões, é preciso avaliar o custo de uma política de securitização em face do desejado avanço tecnológico.

5. À GUISA DE CONCLUSÃO

A IoT é uma realidade. A sua aplicação alcança diversas áreas – saúde, transporte, segurança – com as mais diversas finalidades (consumo, lazer, comércio).

De outro lado, não se pode desconsiderar a possibilidade de prejuízos decorrentes de falhas dos dispositivos, da programação, do sistema, da rede, do programador, enfim, interferências internas e externas. E, ainda, a potencialidade de resultados prejudiciais cuja autoria não seja ou não possa ser identificada.

A tendência contemporânea de reparação/compensação/punição dos danos, a despeito da identificação – ou não – da autoria e/ou da análise do nexo de causalidade, não pode significar o afastamento de toda uma construção e de uma prática do denominado direito dos danos. O problema pode ser novo – as externalidades negativas da IoT –, mas a resposta é antiga: responsabilidade civil – instituto que se renova em face dos novos desafios, que dialoga com mecanismos de regulação e de autorregulação.

Igualmente, é preciso pensar e implementar a regulação sem inibir ou coibir a

31. MUÑOZ, Jesús Jimeno. *Responsabilidad civil em el ámbito de los ciberrriesgos.* Madrid: Fundación Mapfre, 2017, p. 129-130.

32. ALABART, Silvia Díaz. *Robots y responsabilidade civil.* Madrid: Reus editorial, 2018, p. 86.

inventividade e a inovação tecnológica.

A responsabilidade civil pelo implemento da IoT não tem regime jurídico único. A sua aplicação e a sua finalidade ensejam construções e respostas específicas em dinâmico diálogo com regras e princípios conhecidos.

REFERÊNCIAS

ALABART, Silvia Díaz. *Robots y responsabilidade civil.* Madrid: Reus editorial, 2018.

BARBOSA, Pedro Marcos Nunes. *Direito civil da propriedade intelectual:* o caso da usucapião de patentes. 3. ed. Rio de Janeiro: Lumen Juris, 2016.

BITTAR, Eduardo C. B. O direito na era digital: responsabilidade civil e penal pelo uso indevido das redes sociais. In.: SARLET, Ingo Wolfgang; SARLET, Gabrielle B. Sales; BITTAR, Eduardo C.B. *Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital.* São Paulo: Expressa Jur, 2022, p. 15-37.

BRAGA NETTO, Felipe; ROSENVALD, Nelson; FARIAS, Cristiano Chaves. *Novo tratado de responsabilidade civil.* 2. ed. São Paulo: SaraivaJur, 2017.

BRANT, Cássio Augusto Barros. *Usucapião na propriedade intelectual.* Belo Horizonte: D'Plácido, 2014.

CARRÁ, Bruno Leonardo Câmara. *Responsabilidade civil sem dano:* uma análise crítica. Limites epistêmicos a uma responsabilidade civil preventiva ou por simples conduta. São Paulo: Atlas, 2015.

CAVALIERI FILHO, Sergio. *Programa de responsabilidade civil.* 11. ed. São Paulo: Atlas, 2014.

GENNARI, Francesca. What liability with the internet of things ? Insights from the european case-law of the pip affair. Journaul Global jurist. Disponível em: <https://doi.org/10.1515/gj-2022-0032>. Acesso em: 23 de março de 2023.

GODOY, Cláudio Luiz Bueno de. *Responsabilidade civil pelo risco da atividade.* São Paulo: Saraiva, 2009.

GOMES, José Jairo. *Responsabilidade e eticidade.* Belo Horizonte: Del Rey, 2005.

GONÇALVES, Carlos Roberto. *Responsabilidade civil.* 11. ed. São Paulo: Saraiva, 2009.

MARTINS-COSTA, Judith. Usucapião de coisa incorpórea: breves notas sobre um velho tema sempre novo. In.: TEPEDINO, Gustavo; FACHIN, Luiz Edson (Coords). *O direito e o tempo:* embates jurídicos e utopias contemporâneas: estudos em homenagem ao Professor Ricardo Pereira Lira. Rio de Janeiro: Renovar, 2008, p. 631-653.

MILAGRES, Marcelo de Oliveira. A robótica e as discussões sobre a personalidade eletrônica. In.: EHRHARDT JR., Marcos; CATALAN. Marcos; MALHEIROS, Pablo (Org.). *Direito civil e tecnologia*. Belo Horizonte: Fórum, 2020, p. 509-518.

MUÑOZ, Jesús Jimeno. *Responsabilidad civil em el ámbito de los ciberrriesgos.* Madrid: Fundación Mapfre, 2017.

PENTEADO, Luciano de Camargo. Que coisa é a coisa? Reflexões em torno a um pequeno ensaio de Carnelutti. *Revista de direito privado,* São Paulo, n. 39, jul./set. 2009, p. 249-258.

PEREIRA, Caio Mário da Silva. *Responsabilidade civil.* 8. ed. Rio de Janeiro: Forense, 1996.

REIS, Paulo Victor Alfeo. *Algoritimos e o direito.* São Paulo: Almedina, 2020.

SARLET, Ingo Wolfgang; SARLET, Gabrielle B. Sales; BITTAR, Eduardo C. B. *Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital.* São Paulo: Expressa Jur, 2022.

SIQUEIRA NETO, José Francisco; MIRANDA, Lorrayne Barbosa; LANNES, Yuri Nathan da Costa. Inteligência artificial e veículos autônomos: aspectos éticos, políticos e jurídicos. In.: FABRI, Andréa Queiroz; Nascimento, Carlos Eduardo do; PINTO, Felipe Chiarello de Souza (Coords). *Compliance and technology law.* Uberlândia: Composer, 2020, p. 223-248.

TAVARES, André Ramos. *O juiz digital:* da atuação em rede à justiça algorítmica. São Paulo: Expressa, 2022.

TEUBNER, Gunther. *Digital personhood?* The status of autonomous software agents in private law. Tradução de Jacob Watson. Société Suisse des Juristes: Ancilla Iuris, 2018.

USTÁRROZ, Daniel. *Responsabilidade civil por ato lícito.* São Paulo: Atlas, 2014.

INDUSTRIAL INTERNET OF THINGS (IIOT) E RESPONSABILIDADE CIVIL POR FATO DA COISA

Eduardo Goulart Pimenta

Doutor e Mestre em Direito Empresarial – UFMG. Professor Associado de Direito Empresarial na UFMG. Professor Adjunto da Faculdade de Direito da PUC/MG. Procurador do Estado de Minas Gerais. Consultor e árbitro.

DOI: https://doi.org/10.59224/dti5.ch4

Resumo: Empresa e tecnologia são duas realidades essencialmente atreladas, de forma que se influenciam reciprocamente e, sem dúvida, acarretam evolução em ambos os campos. Por outro lado, tem se tornado evidente que a relação entre empresa e tecnologia ganhou nova dimensão, tanto em profundidade quanto em amplitude, com a digitalização da economia. O objeto do presente texto é analisar este novo grau de interação entre empresa e tecnologia e como tal realidade pode ser regulada juridicamente, especialmente quando se trata de responsabilização civil por danos causados ao patrimônio ou à pessoa de terceiros.

Palavras-chave: Industrial Internet of Things; responsabilidade civil; fato da coisa.

Abstract: *Company and technology are two inherently interconnected realities that mutually influence and undoubtedly bring about evolution in both fields. On the other hand, it has become evident that the relationship between company and technology has taken on a new dimension, both in depth and breadth, with the digitization of the economy. The purpose of this text is to analyze this new level of interaction between company and technology and how this reality can be legally regulated, especially when it comes to civil liability for damages caused to the property or person of third parties.*

Keywords: *Industrial Internet of Things; civil liability; thing's defect.*

SUMÁRIO: Introdução; 1. Indústria 4.0: a Quarta Revolução Industrial e a IIoT (*Industrial Internet of Things*); 2. Decisões em IIoT como fatos jurídicos de coisas; 3. A responsabilidade civil por fato jurídico de coisa e sua aplicação à IIoT; 4. Instrumentos jurídicos de afetação de patrimônio aos custos e danos decorrentes do funcionamento da IIoT; Conclusão; Referências.

INTRODUÇÃO

Empresa e tecnologia são duas realidades essenciamente atreladas, de forma que se influenciam reciprocamente e, sem dúvida, acarretam evolução em ambos os campos.

Por outro lado, tem se tornado evidente que a relação entre empresa e tecnologia ganhou nova dimensão, tanto em profundidade quanto em amplitude, com a digitalização da economia.

O objeto do presente texto é analisar este novo grau de interação entre empresa e tecnologia e como tal realidade pode ser regulada juridicamente, especialmente quando se trata de responsabilização civil por danos causados ao patrimônio ou à pessoa de terceiros.

1. INDÚSTRIA 4.0: A QUARTA REVOLUÇÃO INDUSTRIAL E A IIOT (*INDUSTRIAL INTERNET OF THINGS*)

A massificação da informática e da internet, a partir do último quarto do Séc. XX e, mais evidentemente, a partir do Séc. XXI, impactou diretamente a forma de exercício da empresa, a ponto de hoje serem disseminadas as expressões "Quarta Revolução Industrial"[1], "Indústria 4.0" e *smart factories*, que, em essência, visam identificar uma realidade, cada vez mais evidente e atual, na qual a produção ou distribuição de bens e serviços (empresa) é exercida fundamentalmente por meio de tecnologias decorrentes da informática ou da internet.

São instrumentos como robótica, inteligência artificial, computação em nuvem, *blockchain*, *smart contracts*, *machine learning* e *big data*, o quais são aplicáveis não

1. "*Ciente das várias definições e argumentos acadêmicos utilizados para descrever as três primeiras revoluções industriais, acredito que hoje estamos no início de uma quarta revolução industrial. Ela teve início na virada do século e baseia-se na revolução digital.*
É caracterizada por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina). As tecnologias digitais, fundamentadas no computador, software e redes, não são novas, mas estão causando rupturas à terceira revolução industrial; estão se tornando mais sofisticadas e integradas e, consequentemente, transformando a sociedade e a economia global".
Schwab, Klaus. *A Quarta Revolução Industrial*. Edipro. Edição do Kindle.

apenas às atividades quotidianas mas também usados como fatores de produção empresarial.

Entre tais instrumentos tecnológicos, um em especial chama a atenção: trata-se da denominada *Internet of things* (IoT) ou, em português, Internet das Coisas.

A expressão Internet das Coisas (IoT) identifica, essencialmente, objetos interconectados através da internet e computação em nuvem capazes de, por meio desta interconexão, receber e emitir instruções a outros dos objetos interconectados, de forma a prover produtos ou serviços aos destinatários da operação[2].

Se a Internet das Coisas (IoT) identifica uma ideia ampla de conexão e instruções mútuas entre objetos, através da internet, há um aspecto mais específico da expressão. Trata-se da *Industrial Intenet of Thing* (IIoT), Internet das Coisas Industriais ou internet das coisas aplicada ao exercício da empresa. Neste caso, a interconexão e troca de instruções entre objetos é estruturada para funcionar como uma cadeia de produção ou distribuição de bens ou serviços.

As chamadas fábricas inteligentes (*smart factories*)[3], ícones da Indústria 4.0, são

---

2. *Atividades comerciais, como transportes, estão melhorando a gestão de frotas com a telemática. Em assistência médica, a IoT está ampliando os conhecimentos e as competências dos médicos e empoderando os pacientes com informações necessárias para gerenciar e prevenir doenças. E as seguradoras estão medindo o comportamento humano e prevendo o comportamento de máquinas para melhor avaliar o custo do risco. Em qualquer lugar que você observe, os equipamentos estão sendo instrumentados para transmitir dados aos proprietários e usuários, a fim de melhorar o negócio e as relações com os clientes.*
   Sinclair, Bruce (2018-06-26). IoT: *Como Usar a "Internet Das Coisas" Para Alavancar Seus Negócios* (Locais do Kindle 312-316). Autêntica Business. Edição do Kindle.
3. *A smart factory is characterized by four intelligent features:*
   • Sensors: these are devices that have the ability to self-organize, learn, and maintain environmental information to analyze behaviors and abilities. Therefore, sensors can make decisions that enable them to adjust to changes in the environment.
   • Interoperability: through interconnection between different devices, coordination between them can be enhanced, allowing flexibility in configuration protocols of the production system.
   • Integration: robots and artificial intelligence (AI) allow smart factories to have a high level of integration among processes. AI, along with the integration of human intellectual capabilities, enables factories to perform analysis and decision making.
   • Virtual reality (VR) techniques: as one of the high-level components of smart factories, VR facilitates human–machine integration by virtualizing manufacturing processes using computers, signal

entendidas como aquelas calcadas em *softwares* e máquinas conectadas umas às outras através da internet e capazes de coletar dados, processá-los por meio de inteligência artificial e, a partir de tais informações, tomarem decisões e fazerem previsões referentes à cadeia produtiva, bem como sobre a qualidade, desempenho e manutenção de produtos.

Um caso que merece citação é o da Titan International Inc., companhia já centenária e que tem na fabricação de rodas e pneus para veículos usados na produção agrícola ou industrial, seu objeto central. Este exemplo se mostra particularmente importante por ser, como dito, uma companhia com mais de um século de fundação e cujo objeto é uma atividade muito anterior a qualquer digitalização ou informatização industrial.

Em conjunto com a Oracle, através da Oracle Iot Cloud[4], todo o maquinário de fabricação, distribuição e entrega dos produtos foi interconectado por computação em nuvem, de modo que o processo de produção e distribuição dos pneus e rodas funciona a partir de modo totalmente digital.

A cadeia produtiva da Titan Inc. passou a ser estruturada em IIoT a partir de cinco áreas-chave, que são a gestão de estoques, processo de fabricação, logística (distribuição e entrega), relações com trabalhadores e finanças (pagamentos e recebimentos).

Um ponto que chama especialmente a atenção está na análise, a partir do processamento de informações obtidas digitalmente, do estado de conservação e condições de uso dos pneus fornecidos pela companhia, de modo a orientar os clientes, antecipadamente, sobre necessidade de manutenção ou troca e, mesmo, fazer remessas de produtos (*on time delivery*) sem que o usuário/comprador precise tomar qualquer providência.

---

processing, animation technology, intelligent reasoning, prediction, and simulation and multimedia technologies.

TAHERA. Kalsoom. RAMZAN. Naeem. AHMED. Shehzad. UR-REHMAN. Masood. *Advances in Sensor Technologies in the Era of Smart Factory and Industry 4.0.* Sensors 2020, 20, 6783; doi:10.3390/s20236783.

4. ORACLE. *Titan International Case Study*. Sep. 2020. Disponível em: *https://www.oracle.com/br/internet-of-things/*

Por meio de IIoT a Titan International Inc. consegue monitorar digitalmente sua cadeia produtiva além de, com tais informações, aliadas à inteligência artificial, obter maximização de matéria prima, redução de uso energético e maior segurança para trabalhadores, já que cada ponto de risco na cadeia produtiva é digitalmente processado e minimizado.

Entre as várias vantagens do uso da IIoT no exercício da empresa tem-se, de forma mais evidente e direta, a redução no desperdício de matérias primas e consumo de energia (e, consequentemente, maior sustentabilidade ambiental), a maximização no uso do maquinário (reduzindo períodos de subprodução ou inatividade), a redução da inadimplência (posto que os pagamentos são também através de IIoT) e, como dito, o aumento na segurança para os trabalhadores.

Além disso, é possível apontar outro aspecto positivo que a adoção da IIoT indiretamente provoca no exercício da empresa. Ao transferir a tomada de decisões referentes ao exercício da empresa para este complexo de aparelhos interconectados, são reduzidos a zero os conflitos de agência entre os interesses dos tomadores de decisão e daqueles que, espera-se, sejam beneficiados pelo resultado da decisão tomada[5].

Há que se fazer, neste ponto, uma fundamental ponderação: aparelhos interconectados à internet e que executam instruções diante de certos estímulos previamente obtidos é, até este momento da análise, uma questão tecnológica que pouco ou nada parece afetar a necessidade de revisão da literatura sobre obrigações, contratos e responsabilidade civil.

Radicalmente diferente é o tema se suscitada a dúvida sobre a quem se poderá atribuir responsabilidade em caso de danos causados a terceiros - sejam eles fornecedores, trabalhadores ou clientes - em uma cadeia produtiva na qual todo o processo é monitorado e executado sem que ocorram decisões tomadas por humanos.

Para esta abordagem é necessário, em primeiro lugar, verificar qual a natureza jurídica das decisões tomadas, por inteligência artificial, em *smart factories* e, mais especificamente, se o instituto do contrato se aplica a estas transações realizadas em

5. Sobre conflitos e custos de agência, confira: PIMENTA. Eduardo Goulart. *Direito Societário*. 4ª edição. Belo Horizonte. Ed. Expert. 2023. Pg. 421 e seg.

um ambiente empresarial de IIoT.

2. DECISÕES EM IIOT COMO FATOS JURÍDICOS DE COISAS

Decisão é a escolha entre duas ou mais alternativas reciprocamente excludentes. É algo que se efetiva objetivamente, no mundo dos fatos. Um aparelho eletrônico pode, sem dúvida, tomar decisões (ou seja, escolher) a partir de informações a ele disponibilizadas e critérios previamente fornecidos.

Esta realidade já é frequente em um amplo rol de situações sociais e econômicas que vão desde *softwares* que realizam investimentos no mercado de valores mobiliários até aparelhos de ar condicionado que começam a funcionar, sem comandos dados por humanos, em determinadas horas do dia e adaptam sua temperatura às informações extraídas do ambiente.

Esta constatação, porém, é muito diferente de se cogitar que tais aparelhos ou instrumentos digitais emitam ou mesmo possuam *vontade*, elemento essencial à existência do contrato.

Vontade é algo inerente ao ser humano, algo correspondente aos seus desejos, os quais, por sua vez, são formados por inúmeros fatores, muitos dos quais desconhecidos pelo próprio autor da vontade[6]. Ser capaz de tomar decisões não torna aparelhos ou aplicativos elementos capazes de ter ou expressar *vontade* e, portanto, de contratar. Inteligência artificial toma decisões, mas não tem vontade própria. Não deseja, apenas age.

Aparelhos não têm vontade mas fazem escolhas (ou seja, tomam decisões) a partir de critérios e dados obtidos (*big data*) e processados segundo determinados critérios previamente estipulados (*machine learning*).

Sob outra perspectiva, pode-se argumentar que, em IIoT, as decisões executadas nas diferentes fases da cadeia produtiva seriam contratos atribuíveis, juridicamente, aos sujeitos de direito titulares das *smart factories* orientadas ao exercício da empresa.

Por este prisma, quando um aplicativo usado pela Titan International Inc. emite

6. Objeto de estudo em campos que vão da psicologia e psicanálise até a filosofia – seja do Direito ou não - a formação e expressão da vontade é, também, objeto de regulação jurídica, como se pode constatar, por exemplo, face ao instituto do contrato.

uma ordem de compra a um fornecedor de matéria-prima e realiza o pagamento por meio eletrônico, seria possível atribuir à companhia a posição de "contratante" em tal transação.

Entretanto, esta interpretação afigura-se excessivamente extensiva, posto que somente com exagerado esforço interpretativo a operação descrita no parágrafo acima pode ser considerada um contrato e, ainda mais, no qual a companhia Titan International Inc. seja uma das contratantes, ou seja, uma das autoras da *declaração de vontade* necessária à realização do vínculo.

O contrato é um instituto constituído essencialmente por um acordo de vontades. Deste modo, não há como considerar o fato de um aparelho que, segundo estímulos previamente informados, toma e executa uma decisão direcionada a outro aparelho possa ser compreendido como *contrato*, no sentido jurídico da palavra.

Aparelhos – ainda que caracterizados como inteligência artificial - não contratam, mas, como aptos a tomar e, principalmente, implementar decisões, são capazes de provocar *fatos jurídicos*, entendidos aqui como acontecimentos dos quais resultam, ou podem resultar, consequências jurídicas[7].

Deste modo, decisões tomadas – e, principalmente, efetivadas – sem intervenção humana, em ambientes de IIoT são, sob o ponto de vista jurídico, *fatos jurídicos de coisas* definição que não é nova nem no direito nem na legislação civil, como se demonstrará.

Necessário acrescentar também que, mesmo estruturada a partir de tecnologias como *machine learning* e inteligência artificial, as *smart factories* são, juridicamente, estabelecimentos (art. 1. 142 do Código Civil), posto que complexos de bens (móveis, imóveis ou incorpóreos) organizados para o exercício da empresa e, como tais, sujeitos à titularidade de uma ou mais pessoas físicas ou jurídicas.

Desta forma, embora a regular operação destas *smart factories* não se configure como "feixe de contratos" (na linguagem de Ronald Coase[8]) e sim como uma

7. "*Fato jurídico é, pois, o fato ou complexo de fatos sobre o qual incidiu a regra juridica; portanto, o fato de que dimana, agora, ou mas tarde, talvez condicionalmente, ou talvez naõ dimane, eficácia jurídica".* PONTES DE MIRANDA. Tratado de Direito Privado. Vol I. Ed. Revista dos Tribunais. São Paulo. Pg. 77.

8. COASE. Ronald. The Nature of the Firm. *The Firm, The Market and The Law*. Chicago University

sucessão interconectada de *fatos jurídicos de coisas*, a organização dos elementos materiais e imateriais que compõem *smart factories* e as fazem funcionar são atribuíveis a uma determinada pessoa física ou jurídica.

No exemplo da Titan International Inc., embora não seja possível chamar de contratos as decisões tomadas e implementadas via IIoT, não resta dúvidas de que a companhia em questão (Titan International Inc.) é a titular e responsável pela organização do complexo patrimonial/empresarial estruturado a partir de IIoT.

Vale ponderar que o debate sobre a titularidade sobre *smart factories* e a natureza das decisões tomadas em IIoT – muitas vezes equivocadamente chamadas de contratos - somente ganha relevância, sob o aspecto jurídico, em virtude das prestações decorrentes da implementação destas decisões e, mais do que isso, da responsabilidade decorrente delas.

O exercício da empresa, entendida como atividade economicamente organizada para a produção ou distribuição de bens ou serviços implica decisões das quais, em regra, advém custos e, possivelmente, danos.

Custos são compreendidos, neste contexto, como a contraprestação necessária à obtenção de um determinado fator de produção. Para a obtenção de matéria-prima é necessário pagar ao fornecedor, assim como salários são devidos, pelo trabalho prestado, aos empregados e juros são decorrência da captação do dinheiro de terceiros.

Nos ambientes IIoT, instrumentos como *smart contracts*, computação em nuvem e *blockchain* permitem que também o adimplemento destes custos seja implementado sem necessidade de ação ou intervenção humana.

Em casos como o da Titan International Inc., as decisões tomadas e executadas via IIoT têm seus custos igualmente adimplidos também por meio de decisões tomadas e implementadas sem condutas humanas, algo inerente à generalidade das operações com "contratos autoexecutáveis" (*smart contracts)*.

Diferente, entretanto, é a situação referente a possíveis danos decorrentes do funcionamento destas *smart factories,* estruturadas a partir de IIoT. Danos são decorrência de atos ilícitos e geram, para a pessoa ou grupo vítima do dano, o direito à

Press. 1990. Pg. 33 e seg.

reparação dos prejuízos causados.

Posto que, em IIoT, não se pode falar em contrato como instrumento juridico através do qual se realiza a cadeia produtiva – e, sim, fatos jurídicos de coisas - é preciso definir sob qual fundamento e a quem seria possível responsabilizar na hipótese de danos causados pelas decisões tomadas, sem intervenção humana, nestas *smart factories*.

De imediato se percebe que não é possível abarcar, tal dever de reparação sob o prisma de uma responsabilidade contratual, dado inexistir, como já exposto, contrato em cadeias produtivas estruturadas em IIoT.

Resta, deste modo, o recurso às modalidades de responsabilidade civil extracontratuais e, entre elas, uma de ainda incipiente estudo no direito brasileiro e, mais do que isso, disciplinada de forma apenas pontual no Código Civil de 2002. Trata-se da responsabilidade civil por fato de coisa.

3. A RESPONSABILIDADE CIVIL POR FATO JURÍDICO DE COISA E SUA APLICAÇÃO À IIOT

A responsabilidade civil por fato de coisa – ou, melhor, fato *jurídico*[9] de coisa - tem como premissa básica de aplicação a ideia de que *o proprietário responde por tudo o que é seu*. Danos ao patrimônio ou à pessoa de terceiros podem ser provocados não apenas por condutas humanas, mas também por consequências de fatos decorrentes de coisas.

É possível apontar no art. 1.384 do Código Civil Francês de 1804 a original referência normativa à premissa acima referida, pois tal dispositivo estipula, literalmente, que "*somos responsáveis não somente pelos danos provocados por nossa própria culpa, mas também por aqueles provocados pela culpa das pessoas pelas quais somos responsáveis ou pelas coisas que temos sob nossa guarda*"[10].

9. "*(…) para serem erigidos à categoria de fato jurídico, basta que os fatos do mundo – meros eventos ou condutas – sejam relevantes à vida humana em sua interferência intersubjetiva, independentemente de sua natureza*". MELLO. Marcos Bernardes de. *Teoria do Fato Jurídico*. 5ª edição. Ed. Saraiva. São Paulo. 1993. Pg. 35/36.

10. *Art. 1384. On est responsable non seulement du dommage que l'on cause par son propre fait, mais*

A situação mais evidente é a de um rebanho de gado que, por exemplo, invade a plantação vizinha e a ela danifica. Nítido, neste caso, que o proprietário dos animais deve ser responsabilizado por reparar os prejuízos do agricultor. Igualmente evidente é o caso do proprietário de um imóvel urbano que, por falta de manutenção, se despedaça e provoca danos ao imóvel vizinho.

O Código Civil de 2002 trata da responsabilidade civil por fato jurídico de coisa nos art. 936 a 938 de forma a elencar, expressamente, apenas previsões referentes a fatos provocados por animais ou decorrentes da manutenção de imóveis urbanos.

Já o Código de Defesa do Consumidor, embora mais antigo, cuidou, em seus art. 12 a 17, da responsabilidade civil por fato do produto ou serviço, de modo a imputar responsabilidade em situações de danos causados, ao destinatário final, pelo mal funcionamento de produtos ou execução inadequada de serviços.

Com o aumento da complexidade das organizações empresariais, a ideia de responsabilidade do proprietário, por fatos decorrentes de seu patrimônio, tomou nova dimensão a partir do Séc. XX e certamente será de grande utilidade em face de uma realidade empresarial calcada em *smart factories* e IIoT.

Se, em uma perspectiva anterior à massificação da automação – e, posteriormente, IIoT – no exercício da empresa aventava-se, para fins de responsabilidade civil, somente fatos de animais ou imóveis como fatos jurídicos de coisa, tal limitação não mais se justifica.

Os danos causados pelo animal de alguém ou pela falta de manutenção em um apartamento não são, tanto do ponto de vista fático quanto jurídico, diferentes de danos que venham a ser causados pelo malfuncionamento de uma *smart factory* e das decisões tomadas em IIoT.

Na medida que o empresário ou sociedade empresária (como no caso da Titan

---

encore de celui que est causé par le fait des personnes don't on doit répondre, ou des choses que l'on a sous sa garde. (L. 7 nov. 1922) Toutefois, celui qui détient, à um titre quelconque, tout ou partie de l'immeuble ou des biens mobiliers dans lesquels um incendie a pris naissance ne sera responsable, vis-à-vis des tiers, des dommages causés par cet incendie que s'il est prouvé qu'il doit être attribué à as faute ou à la faute des personnes dont il est responsable. Cette disposition ne s'applique pas aux rapports entre propriétaires et locataires, qui demeurent régis par les articles 1733 et 1734 du code civil. Grifos nossos.

International Inc.) organiza, sob sua titularidade, *smart factory* e permite que decisões sejam tomadas e implementadas por IIoT, torna-se necessário concluir, sob a ótica da responsabilidade civil por fato jurídico de coisa, que os danos causados na tomada ou execução de tais decisões seja atribuível à pessoa deste empresário ou sociedade empresária.

Posto que uma *smart factory* em IIoT é um complexo de bens organizado para o exercício da empresa e, como tal, suscetível de titularidade por parte de pessoa física ou jurídica (empresário individual ou coletivo); que tal complexo de bens é, em sua operação, permeado por uma série de decisões tomadas e implementadas sem intervenção humana (via inteligência artificial); que tais decisões são fatos jurídicos de coisas e que, por fim, tais fatos jurídicos de coisas podem ocasionar danos a terceiros, não se afigura razoável afastar, neste caso, a premissa de responsabilidade segundo a qual *o proprietário responde por tudo o que é seu.*

Deste modo, não se pode compreender como taxativas as hipóteses de responsabilidade civil por fato jurídico de coisa enumeradas pelo Código Civil, sob pena de tratamento jurídico diferente a situações fáticas idênticas[11].

Portanto, a cadeia produtiva estruturada em IIoT e os bens dela componentes estão sob a titularidade do empresário ou sociedade empresária que, face à responsabilidade civil por fato de coisa, é responsável pelos danos eventualmente causados pelas decisões tomadas, em seu ambiente empresarial, sem a intervenção humana.

Acrescente-se que a responsabilidade civil por fato jurídico de coisa é de natureza objetiva e recai sobre o chamado "guardião da coisa", que, por presunção, é o proprietário do bem causador do dano[12].

---

11. "*De fato, a teoria da responsabilidade pela guarda da coisa representa um avanço em torno do princípio da responsabilidade objetiva. Presume-se a responsabilidade do dono da coisa pelos danos por ela ocasionados a terceiros. Somente se elide essa responsabilidade provando-se culpa exclusiva da vítima ou caso fortuito. Essa posição, no curso da história da responsabilidade civil, representa, sem dúvida, palpável avanço em relação à responsabilidade com culpa. O fato é que a responsabilidade pelo fato da coisa, quer vista sob o prisma da culpa presumida do guardião, quer vista sob o prisma da teoria do risco, representa considerável avanço em relação às teorias anteriores, vigentes no século XIX."* VENOSA. Silvio Salvo. *Direito Civil: Obrigações e responsabilidade Civil – Vol. 1.* 9ª edição. 2021. Pg. 392.

12. STOCO, Rui. *Tratado de responsabilidade civil.* 6.ed. São Paulo: Revista dos Tribunais, 2004, p.

Em situações como a da Titan International Inc. é bastante seguro concluir que o guardião daquele complexo patrimonial chamado *smart factory* é a sociedade empresária dele titular, qual seja a companhia Titan International. Entretanto, há situações nas quais a definição sobre a guarda e mesmo quanto à propriedade sobre o complexo IIoT torna-se mais nebulosa, assim como a definição sobre a responsabilidade pela reparação de eventuais danos.

4. INSTRUMENTOS JURÍDICOS DE AFETAÇÃO DE PATRIMÔNIO AOS CUSTOS E DANOS DECORRENTES DO FUNCIONAMENTO DA IIOT

Smart Factories e IIoT desafiam, em última análise, o até agora tido com essencial vínculo entre patrimônio usado para o exercício da empresa e uma pessoa física ou jurídica (o empresário ou sociedade empresária) que dele seja titular.

Um dos pilares do direito empresarial está na tríade empresa-empresário-estabelecimento (art. 966 c/c art. 1. 142 do C.C), sendo a primeira a atividade economicamente organizada para a produção ou distribuição de bens ou serviços, o segundo o sujeito de direito que se dedica a tal atividade e o terceiro o complexo patrimonial organizado e sob a titularidade do empresário com o objetivo de viabilizar, na prática, o exercício da atividade.

Desta forma, tem-se como inafastável a relação entre o complexo patrimonial usado para o exercício da empresa e uma pessoa física ou jurídica (empresário) que dele seja titular e, por causa disso, se responsabilize pelos custos e danos decorrentes do exercício da empresa.

Em situações como a da Titan International Inc., ainda que se fale em *smart factory* e IIoT, a premissa descrita permanece válida e aplicável, posto que a companhia é facilmente identificável como pessoa jurídica titular da *smart factory* e, como demonstrado no item anterior, responsável pelos danos decorrentes da IIoT.

Entretanto, não se afigura distante a perspectiva de uma *smart factory* cuja titularidade não seja atribuível a uma determinada pessoa física ou jurídica uma vez que, por exemplo, sua constituição e capitalização tenha se efetivado, por exemplo, de forma descentralizada e pulverizada, com o uso de operações como *crowdfunding* ou

934.

tokensales.

Nesta hipotética – mas verossímil – situação, torna-se necessário aventar formas de assegurar, em caso de danos causados pelas decisões tomadas e executadas via IIoT, a responsabilização civil pelos fatos jurídicos de tais coisas.

A questão está, portanto, na possibilidade da existência de patrimônio afetado ao exercício da empresa - as *smart factories* - mas sem a identificação de um sujeito de direito como titular e/ou guardião de tal patrimônio e, por consequência, civilmente responsável pelas decisões tomadas em IIoT.

Uma das possíveis respostas para o problema é admitir que terceiros, não vinculados aos benefícios ou às decisões tomadas e executadas na IIoT, possam volutariamente se responsabilizar pelos danos eventualmente causados pela *smart factory*.

É, por exemplo, o caso do seguro, que é, como sabido, um contrato pelo qual o risco de uma determinada operação é transferido do contratante para a seguradora, mediante contraprestação.

O objeto do contrato de seguro é, em síntese, o risco da operação. No caso de decisões tomadas em *smart factories*, por IIoT, o risco a ser garantido pela seguradora são os possíveis danos decorrentes do cumprimento das decisões tomadas por inteligência artificial.

Avançando um pouco mais, pode-se também especular sobre sistemas de financiamento coletivo – como os já citados *crowdfunding* e *tokensales* – através dos quais seria possível agregar patrimônio destinado à responsabilização pelos danos eventualmente causados no funcionamento de IIoT.

Afastadas as alternativas acima, a operação de uma *smart factory,* com decisões em IIoT, mas sem o vínculo com um determinado empresário ou sociedade empresária pode, sem dúvida, representar uma situação na qual seja juridicamente impossível responsabilizar civilmente alguém pelos danos eventualmente decorrentes da atuação da IIoT.

Em hipóteses que tais, um mecanismo interessante de tutela ao interesse de terceiros é a exigência de que seja previamente divulgado, nas operações da *smart factory* em IIoT, que a mesma não está vinculada a uma determinada pessoa física ou jurídica.

Esta alternativa já é discutida, no mercado de valores mobiliários, como forma de regulação das operações realizadas por *softwares* "robôs". Chamada de *flagging*, teria, no caso, o objetivo de "alertar" terceiros para que estes fiquem previamente cientes de que estão diante de uma *smart factory* na qual decisões são tomadas por meio de IIoT e, além disso, não vinculada a um empresário ou sociedade empresária ao qual seja possível responsabilizar civilmente por eventuais danos.

CONCLUSÃO

Smart factories e *IIOT* são realidades inafastáveis e, mais do que isso, ainda incipientes, já que tendem, em futuro próximo, a se tornar exponencialmente mais comuns.

Cabe ao Direito regular a operação de tais *smart factories* de forma a, principalmente, preservar o interesse de terceiros que possam, direta ou indiretamente, sofrer danos em sua pessoa ou patrimônio.

Para fins desta regulação, fica claro que a responsabilidade civil objetiva por fatos jurídicos de coisas se mostra não apenas adequada mas plenamente aplicável.

REFERÊNCIAS

COASE. Ronald. The Nature of the Firm. *The Firm, The Market and The Law*. Chicago University Press. 1990.

MELLO. Marcos Bernardes de. *Teoria do Fato Jurídico*. 5ª edição. Ed. Saraiva. São Paulo. 1993.

PIMENTA. Eduardo Goulart. *Direito Societário*. 4ª edição. Belo Horizonte. Ed. Expert. 2023.

PONTES DE MIRANDA. Tratado de Direito Privado. Vol I. Ed. Revista dos Tribunais. São Paulo.

SCHWAB, Klaus. *A Quarta Revolução Industrial* . Edipro. Edição do Kindle.

SINCLAIR, Bruce (2018-06-26). IoT: *Como Usar a "Internet Das Coisas" Para Alavancar Seus Negócios* (Locais do Kindle 312-316). Autêntica Business. Edição do Kindle.

STOCO, Rui. ***Tratado** de responsabilidade **civil.*** 6.ed. São Paulo: Revista dos Tribunais, 2004, p. 934.

TAHERA. Kalsoom. RAMZAN. Naeem. AHMED. Shehzad. UR-REHMAN. Masood. *Advances in Sensor Technologies in the Era of Smart Factory and Industry 4.0.* Sensors 2020, 20, 6783; doi:10.3390/s20236783.

VENOSA. Silvio Salvo. *Direito Civil: Obrigações e responsabilidade Civil – Vol. 1.* 9ª edição. 2021.

O REGISTRO PRÉVIO PARA O EXERCÍCIO PROFISSIONAL DE ATIVIDADES ENVOLVENDO TECNOLOGIAS E SISTEMAS:

UMA ANÁLISE SOBRE OS BENEFÍCIOS E MALEFÍCIOS QUE A EXIGÊNCIA DE AUTORIZAÇÃO PRÉVIA PODERIA TRAZER AO MERCADO DE TECNOLOGIA DA INFORMAÇÃO SOB O PONTO DE VISTA DA LIVRE INICIATIVA

Vívian Costa Marques

Mestranda em Direito pela Universidade Federal de Minas Gerais (UFMG), área P-08 (negócios no sistema financeiro nacional – tutela penal e administrativa). Pós-graduada em Direito das sucessões pela EBRADI. Especialista em Investimentos pela ANBIMA (CEA). Advogada.

DOI: https://doi.org/10.59224/dti5.ch5

Resumo: Este artigo questiona se a exigência de autorização prévia estatal para o exercício das atividades envolvendo a prestação de serviços de tecnologia e desenvolvimento de sistemas fere os princípios constitucionais da ordem econômica, e, em especial, da livre iniciativa. Para isso, analisa os Decretos existentes sobre a internet das coisas e iniciativas para a transformação digital, bem como o fundamento constitucional para a existência da regulação sobre essas atividades com exigência de registro prévio para o exercício dessas profissões. Por fim, traça um comparativo dos benefícios e malefícios que isso poderia trazer ao mercado de tecnologia da informação sob o ponto de vista da livre iniciativa e fomento da inovação.

Palavras-chave: regulação de atividades econômicas; prévia autorização; prestação de serviços de tecnologia e programação.

Abstract: *This article if the requirement of prior state authorization for the special exercise of technology concession activities and systems development offers the constitutional, economic and free enterprise principles. For this, we analyzed the existing Decrees on the internet of things and initiatives for digital transformation, as well as the constitutional one for the existence of regulation on these activities with a requirement of prior registration for the exercise of these professions. Finally, a comparison of the benefits and harms that this can bring to the information technology market from the point of view of free enterprise and fostering innovation.*

Keywords: *regulation of economic activities; prior authorization; provision of technology and programming services.*

1. INTRODUÇÃO

A autorização prévia para o exercício de atividades econômicas é tema que gera debate, principalmente quando observado o princípio da livre iniciativa para o sujeito empreender e o interesse do Estado em limitar o desenvolvimento de determinadas atividades. No Brasil, em que pese a existência de órgãos reguladores e exigência de registro prévio para os mais diversos mercados, não existe uma regulação específica para o desenvolvimento das atividades dos profissionais de tecnologia e sistemas, termo que será utilizado neste artigo para se referir aos diversos agentes que programam e desenvolvem sistemas, softwares e lidam com outros recursos envolvendo a linguagem computacional, tema sobre o qual este artigo irá tratar.

A pergunta proposta questiona se a exigência de autorização prévia estatal para o exercício dessas atividades citadas fere os princípios constitucionais da ordem econômica, e, em especial, da livre iniciativa.

Para desenvolver o estudo, o autor irá abordar brevemente o histórico do desenvolvimento da tecnologia da informação, bem como os Decretos existentes que dizem respeito à inovação na economia digital, relacionando-os com os interesses públicos que porventura poderiam ser utilizados como justificativa para existência de um órgão regulador específico para a área.

Em seguida, irá conceituar a expressão regulação, com enfoque na perspectiva constitucional e legislativa para fundamentar a exigência de registro prévio para o desenvolvimento de atividades econômicas, explicando como isso seria aplicável aos profissionais da tecnologia da informação.

Posteriormente, será traçado um breve comparativo entre os pontos positivos e

negativos que a e eventual barreira de acesso ao mercado da tecnologia da informação pode trazer à população e ao desenvolvimento de novos negócios baseado na internet e internet das coisas.

Por fim, a hipótese formulada, de que a existência de registro prévio para o desenvolvimento das atividades mencionadas não fere os princípios da livre iniciativa será confirmado, mas desde que haja uma lei específica dispondo sobre essa possibilidade e o cumprimento de outros requisitos legais, conforme se verá adiante.

2. BREVE HISTÓRICO DA TECNOLOGIA DA INFORMAÇÃO E O SURGIMENTO DE NOVOS NEGÓCIOS E PROFISSÕES RELACIONADAS

Conceituar ou estabelecer quem são os profissionais que lidam com a tecnologia e sistemas não é tarefa fácil. Em um ambiente extremamente dinâmico e disruptivo, o profissional que lida de alguma forma com essas duas áreas pode ser chamado de diversas formas, bem como ocupar diversos cargos ou funções, dentre elas: analista de sistemas; analista de banco de dados; desenvolvedor de programas; arquiteto ou engenheiro de softwares; programador; desenvolvedor; profissional de tecnologia da informação, dentre outros.

O contexto histórico em que surgiram os primeiros profissionais não é certo, mas certamente está relacionado ao surgimento da internet e ao abandono do simples processamento de dados para o avanço da informática. Segundo Rezende[1]:

> (...) na década de 1960, o tema tecnológico que rondava as organizações era o "processamento de dados". Nessa época, a maioria das empresas direcionava os recursos para o processamento centralizado de dados em mainframes (grandes computadores) e para os sistemas de controles operacionais, tais como faturamento, estoque, folha de pagamento, finanças e contabilidade. (...) Aos poucos, porém, as empresas foram se sensibilizando para a importância da informação na gestão de negócios. (...) Com a "informática", as empresas integraram os seus sistemas, mesmo com algumas redundâncias. Na atualidade, a "informática" se transforma em "tecnologia da informação" (TI), integrando os seus emergentes e modernos recursos. A TI pode ser conceituada como o conjunto dos recursos tecnológicos e computacionais para guarda

1. REZENDE, Denis Alcides. Evolução da Tecnologia da Informação nos últimos 45 anos. Revista FAE Business, v. 4, p. 42-46, 2002.

> de dados, geração e uso da informação e de conhecimentos. (...) Com a "tecnologia da informação" as empresas possuem aplicações com compartilhamento das bases de dados, unificando-as e eliminando as redundâncias. Os sistemas são mais completos, integrados e satisfazem na íntegra os seus usuários. A TI contempla inclusive os sistemas de informação e de conhecimento para apoio às decisões. Dessa forma, utilizando a TI, a informação e o conhecimento adicionam para as organizações diversas facilidades de gestão com vantagens competitivas e com inteligência empresarial.

Ou seja, se antes o foco era o processamento de dados e manuseio das informações, depois o objetivo foi o "*desenvolvimento de sistemas gerenciais e sistemas estratégicos capazes de trabalhar não apenas com dados, mas com a geração de informação e de conhecimento*"[2], alcançado por meio da prestação de serviços profissionais qualificados com *expertise* em tecnologia e sistemas.

Atualmente, pode-se afirmar que o negócio evoluiu para um modelo ainda mais tecnológico e interligado, haja vista o surgimento da *internet of thing* (IoT), ou internet das coisas, termo definido pelo Decreto n. 9.854 de 2019 como "*a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade.* "[3] De forma mais simples,

> A Internet das Coisas, em poucas palavras, nada mais é que uma extensão da Internet atual, que proporciona aos objetos do dia-a-dia (quaisquer que sejam), mas com capacidade computacional e de comunicação, se conectarem à Internet. A conexão com a rede mundial de computadores viabilizará, primeiro, controlar remotamente os objetos e, segundo, permitir que os próprios objetos sejam acessados como provedores de serviços. Estas novas habilidades, dos objetos comuns, geram um grande número de oportunidades tanto no âmbito acadêmico quanto na indústria.[4]

Com certeza, além dos profissionais de tecnologia da informação, toda a

2. DE SOUZA, Élida Patrícia. CARREIRA EM TECNOLOGIA DA INFORMAÇÃO: um estudo junto a profissionais de Minas Gerais. Tese apresentada ao Centro de Pós Graduação e Pesquisas em Administração da Universidade Federal de Minas Gerais, como requisito parcial para a obtenção do título de Doutorado em Administração. Belo Horizonte, 2018. P. 56.
3. BRASIL. Presidência da República. Decreto n. 9.854, de 25 de junho de 2019. Art. 2º, I.
4. SANTOS, Bruno P. SILVA, Lucas A. M; CELES, Clayson S. F. S; NETO, João B. Borges; PERES,

população será impactada com a chegada de dispositivos interligados pela internet das coisas, o que entrou no radar em um Plano Nacional do Governo instituído pelo Decreto n. 9.854 de 2019. Neste sentido, e para melhor compreender a importância do assunto para os profissionais que lidam com tecnologia e sistemas, veja-se os objetivos do Plano e a delimitação dos temas que o integram, para identificação de soluções para viabilizá-lo:

> "Art. 3º São objetivos do Plano Nacional de Internet das Coisas:
> I - melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT;
> **II - promover a capacitação profissional relacionada ao desenvolvimento de aplicações de IoT e a geração de empregos na economia digital;**
> III - incrementar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT, por meio da promoção de um ecossistema de inovação neste setor;
> IV - buscar parcerias com os setores público e privado para a implementação da IoT; e
> V - aumentar a integração do País no cenário internacional, por meio da participação em fóruns de padronização, da cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de IoT desenvolvidas no País.
> (...)
> Art. 5º Ficam estabelecidos os seguintes temas que integrarão plano de ação destinado a identificar soluções para viabilizar o Plano Nacional de Internet das Coisas
> **I - ciência, tecnologia e inovação;**
> II - inserção internacional;
> **III - educação e capacitação profissional;**
> IV - infraestrutura de conectividade e interoperabilidade;
> **V - regulação, segurança e privacidade; e**
> **VI - viabilidade econômica.**
> Parágrafo único. As ações desenvolvidas no plano de ação de que trata o caput deverão estar alinhadas com as ações estratégicas definidas na Estratégia Brasileira para a Transformação Digital, nos termos do disposto no Decreto nº 9.319, de 21 de março

Bruna S; VIEIRA, Marcos Augusto M.; Vieira, Luiz Filipe M.; Goussevskaia Olga N; LOUREIRO, Antonio A. F.- Internet das Coisas: da Teoria à Prática. Departamento de Ciência da Computação Universidade Federal de Minas Gerais (UFMG) Belo Horizonte, 2019.

de 2018."[5] **(grifo nosso)**

Pela leitura em conjunto dos incisos destacados acima, é possível afirmar que o Decreto abre espaço para uma possível regulação mais detalhada no futuro, haja vista a expressa preocupação com a capacitação profissional do sujeito que irá lidar com toda a tecnologia e os esforços para a geração de empregos na economia digital.

Entretanto, o intuito do Decreto não foi limitar a atividade, exigindo requisitos ou impondo deveres para o exercício regular, mas sim, estimular a inovação, assim como no Decreto n. 9.319, de 21 de março de 2018, que instituiu o Sistema Nacional para a Transformação Digital e estabeleceu a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital (E-digital). Conforme disposto no Decreto,

> "(...) § 1º A E-Digital, fundamentada nos eixos temáticos constantes do Anexo I a este Decreto, visa à harmonização das iniciativas do Poder Executivo federal ligadas ao ambiente digital, com o objetivo de aproveitar o potencial das tecnologias digitais para promover o desenvolvimento econômico e social sustentável e inclusivo, com inovação, aumento de competitividade, de produtividade e dos níveis de emprego e renda no País.
>
> § 2º A E-Digital será estruturada conforme os seguintes eixos temáticos:
>
> I - eixos habilitadores:
>
> a) infraestrutura e acesso às tecnologias de informação e comunicação: objetiva promover a ampliação do acesso da população à internet e às tecnologias digitais, com qualidade de serviço e economicidade;
>
> b) pesquisa, desenvolvimento e inovação: objetiva estimular o desenvolvimento de novas tecnologias, com a ampliação da produção científica e tecnológica, e buscar soluções para desafios nacionais;
>
> **c) confiança no ambiente digital: objetiva assegurar que o ambiente digital seja seguro, confiável, propício aos serviços e ao consumo, com respeito aos direitos dos cidadãos;**
>
> **d) educação e capacitação profissional: objetiva promover a formação da sociedade para o mundo digital, com novos conhecimentos e tecnologias avançadas, e prepará-la para o trabalho do futuro; e**
>
> e) dimensão internacional: objetiva fortalecer a liderança brasileira nos fóruns globais relativos a temas digitais, estimular a competitividade e a presença das empresas

5. BRASIL. Presidência da República. Decreto n. 9.854, de 25 de junho de 2019. Art. 3º.

brasileiras no exterior, e promover a integração regional em economia digital; e

II - eixos de transformação digital:

a) transformação digital da economia: objetiva estimular a informatização, o dinamismo, a produtividade e a competitividade da economia brasileira, de forma a acompanhar a economia mundial; e

b) cidadania e transformação digital do Governo: tornar o Governo federal mais acessível à população e mais eficiente em prover serviços ao cidadão, em consonância com a Estratégia de Governo Digital. *(Redação dada pelo Decreto nº 10.332, de 2020)*

§ 3º A E-Digital será disciplinada em ato do Ministro de Estado da Ciência, Tecnologia e Inovações e servirá de referência para o SinDigital. *(Redação dada pelo Decreto nº 10.782, de 2021)*"[6] **(grifo nosso)**

Em verdade, o que se pretende com a educação e capacitação profissional acima negritada é a promoção do amplo acesso de "*alunos e professores a recursos didáticos de qualidade e possibilitar práticas pedagógicas inovadoras, por meio da disseminação do acesso à internet de alta velocidade em escolas públicas*"[7], bem como o aprimoramento das "*capacidades técnicas e humanas relativas ao uso e tratamento de grandes volumes de dados*"[8] para fins de preparação da própria sociedade e dos profissionais para a transformação digital da economia baseada em dados, há vista que "*o aproveitamento das oportunidades advindas da crescente disponibilidade do grande volume*

6. BRASIL. Presidência da República. Decreto n. 9.319, de 21 de março de 2018. Art. 1º, § 1º.
7. BRASIL. Presidência da República. Decreto n. 9.319, de 21 de março de 2018. *ANEXO I. EIXOS TEMÁTICOS DA ESTRATÉGIA BRASILEIRA PARA A TRANSFORMAÇÃO DIGITAL - E-DIGITAL. I - Eixos habilitadores. 4. Educação e capacitação profissional. No campo educacional, deve-se promover o amplo acesso de alunos e professores a recursos didáticos de qualidade e possibilitar práticas pedagógicas inovadoras, por meio da disseminação do acesso à internet de alta velocidade em escolas públicas. Os objetivos a serem alcançados incluem: - conectar escolas públicas, urbanas e rurais, com acessos de banda larga, e disponibilizar equipamentos para acesso a tecnologias digitais; - incorporar as tecnologias digitais nas práticas escolares, com desenvolvimento do pensamento computacional entre as competências dos estudantes; - reforçar as disciplinas matemática, ciências, tecnologias e engenharias e as trilhas de formação técnica para atuação em setores da economia digital, com foco no empreendedorismo; e - promover o aprimoramento das formações inicial e continuada dos professores, no que se refere ao uso da tecnologia em sala de aula.*
8. BRASIL. Presidência da República. Decreto n. 9.319, de 21 de março de 2018. ANEXO I. EIXOS TEMÁTICOS DA ESTRATÉGIA BRASILEIRA PARA A TRANSFORMAÇÃO DIGITAL - E-DIGITAL. II - Eixos de transformação digital 1. Transformação digital da economia. (a) Economia baseada em dados

de dados é, assim, elemento estratégico para o crescimento do País."[9]

Dessa forma, assim como o aprimoramento das capacidades técnicas e humanas foi pensado como objetivo a ser alcançado para o eixo de transformação digital na economia baseada em dados, a promoção de "*um ambiente jurídico-regulatório que estimule investimentos e inovação, a fim de conferir segurança aos dados tratados e adequada proteção aos dados pessoais"*[10] também foi inserido como um desses objetivos, o que requer atenção. E o Decreto prossegue em evidenciar a preocupação para fomentar tanto o ambiente normativo quanto o ambiente de negócios para promoção da atração de novos investimentos em dispositivos conectados. Neste sentido, veja-se:

> "II - Eixos de transformação digital
> 1. Transformação digital da economia
> (a) Economia baseada em dados
> (...)
> (b) Um Mundo de Dispositivos Conectados
> Ao reconhecer o potencial transformador das aplicações da Internet das Coisas, devem ser estabelecidos ações e incentivos destinados à contínua evolução e disseminação dos dispositivos e das tecnologias digitais associadas.
> Os objetivos a serem alcançados incluem:
> - apoiar a formação e a capacitação profissional em habilidades necessárias para o desenvolvimento e a utilização das novas tecnologias digitais relacionadas aos dispositivos conectados;
> - promover o desenvolvimento de soluções tecnológicas nas áreas prioritárias de saúde, agropecuária, indústria e cidades inteligentes; e
> **- fomentar o ambiente normativo e de negócios que promova a atração de novos investimentos em dispositivos conectados, a fim de assegurar a confiança e a**

9. BRASIL. Presidência da República. Decreto n. 9.319, de 21 de março de 2018. ANEXO I. EIXOS TEMÁTICOS DA ESTRATÉGIA BRASILEIRA PARA A TRANSFORMAÇÃO DIGITAL - E-DIGITAL. II - Eixos de transformação digital 1. Transformação digital da economia. (a) Economia baseada em dados.
10. BRASIL. Presidência da República. Decreto n. 9.319, de 21 de março de 2018. ANEXO I. EIXOS TEMÁTICOS DA ESTRATÉGIA BRASILEIRA PARA A TRANSFORMAÇÃO DIGITAL - E-DIGITAL. II - Eixos de transformação digital 1. Transformação digital da economia. (a) Economia baseada em dados

preservação de direitos dos usuários; e

(c) Novos Modelos de Negócio

O ambiente digital, em especial aquele viabilizado pela internet, reduz barreiras de entrada, gera novos mercados e viabiliza o surgimento de modelos de negócios disruptivos. Ao mesmo tempo, a velocidade das transformações exige de reguladores e formuladores de políticas agilidade e flexibilidade na criação de um ambiente de negócios competitivo e propício ao desenvolvimento da economia digital.

Os objetivos a serem alcançados incluem:

- reforçar a atuação de empresas brasileiras no ambiente de negócios digital;
- estimular e apoiar empresas nascentes de base tecnológica; e
- **desenvolver ambientes regulatórios flexíveis para experimentação de modelos de negócios inovadores.**"[11]

Decerto, desenvolver ambientes com novos modelos de negócio e eventualmente desenvolver uma regulação flexível para experimentação destes não é tarefa fácil, principalmente quando a preservação dos direitos dos usuários é colocada em pauta, o que enseja a atuação do Estado em sua medida certa, tarefa da regulação.

3. A REGULAÇÃO ESTATAL COMO INSTRUMENTO DE INTERVENÇÃO INDIRETA NA ECONOMIA

Antes de conceituar o que é regulação, cumpre relembrar o contexto histórico do surgimento desse instrumento de intervenção indireta na economia. Segundo Paulo Bonfadini[12],

> (...) a rápida evolução da economia e da tecnologia ao longo principalmente do século XX – algo como um legado da revolução industrial e do liberalismo pós revolução francesa -, fez com que as atividades econômicas se diversificassem muito. Várias foram as atividades que surgiram no mundo. Tão variadas que o estado social – aquele que exercia as atividades econômicas com vistas a custear e materializar os direitos sociais, ditos "prestacionistas" – teve de sair de cena. A diversificação da econômica

11. BRASIL. Presidência da República. Decreto n. 9.319, de 21 de março de 2018. *ANEXO I. EIXOS TEMÁTICOS DA ESTRATÉGIA BRASILEIRA PARA A TRANSFORMAÇÃO DIGITAL - E-DIGITAL.* II - Eixos de transformação digital 1. Transformação digital da economia. (b) (c)
12. BONFADINI, Paulo André Espírito Santo. O poder normativo autônomo das agências reguladoras. Critérios e controles. 1ª Ed. Rio de Janeiro: Lumen Juris Editora, 2021. P. 58.

> fez o Estado Social encolher (...) A economia é dinâmica, como se sabe, e o que está em evidência hoje no mercado, amanhã pode não estar mais. Sendo dinâmica a atividade econômica, dinâmica deve ser a atuação do Estado ao regulá-la.

Portanto, pode-se afirmar que foi exatamente esse dinamismo da sociedade e dos mercados que fez com que a regulação se tornasse necessária, em detrimento também do processo legislativo, o qual não consegue acompanhar de perto as transformações da sociedade em razão da sua demora e burocracia para aprovação das leis. A respeito do modo como a regulação se dá, continua:

> O órgão regulador responsável por uma atividade econômica específica deve ter o poder de: executar políticas públicas e econômicas do momento e de longo prazo com mais autonomia técnica e sem maiores intervencionismos político-ideológicos do Poder Público central; julgar os conflitos entre os agentes econômicos ou entre esses e o próprio ente regulador com amplo contraditório e possibilidade de produção de provas, num contexto dialético que se espera não só do processo judicial mas também do processo administrativo (art. 5º, LIV, CF-88); e editar normas técnicas capazes de planejar e regular aquela atividade econômica específica, prevenir conflitos e violações a outros interesses da ordem econômica (meio ambiente, consumidores, terceiros, concorrência) e viabilizar o eficiente exercício da referida atividade pelos agentes econômicos.

Veja-se que a atividade regulatória é dinâmica, pois envolve a criação de normas, sua fiscalização e eventual sanção pelo descumprimento. Para isso, o órgão regulador competente deve ser técnico, bem como se utilizar de mecanismos mais flexíveis e ágeis, em que pese ser quase impossível que a regulação venha a acompanhar, na mesma velocidade, o surgimento de novos negócios da economia digital.

O atual arcabouço regulatório brasileiro de atuação indireta na econômica foi consolidado especificamente no artigo 174 da Constituição Federal, o qual sugere o conceito de regulação como instrumento do Estado para regular determinada atividade, o que envolve a normatização, fiscalização, incentivo e planejamento, impondo limites aos propósitos negociais dos sujeitos e ao desenvolvimento das atividades. De acordo com a Constituição Federal[13],

> Art. 174. Como agente normativo e regulador da atividade econômica, o Estado

13. BRASIL. Constituição Federal. Art. 174.

> exercerá, na forma da lei, as funções de fiscalização, incentivo e planejamento, sendo este determinante para o setor público e indicativo para o setor privado.

Dessa forma, é a própria lei, a qual cria o órgão regulador, que irá definir as competências específicas para execução dos instrumentos regulatórios normativos, executivos e judicantes, conforme objetivos da regulação específica daquele setor. No Brasil, a maioria dos órgãos reguladores foram criados pela lei sob a forma de Autarquias Federais em regime especial, como a Agência Nacional de Energia Elétrica, Agência Nacional de Saúde Suplementar; Agência Nacional de Telecomunicações; Comissão de Valores Mobiliários, dentre vários outros órgãos da Administração Pública indireta espalhados para moldar determinados mercados, operações e profissionais que neles atuam, tudo conforme os princípios gerais da ordem econômica e financeira e fundamentos do Estado.

3.1. A REGULAÇÃO ESTATAL SOBRE AS ATIVIDADES ECONÔMICAS E A LIVRE INICIATIVA

Conforme dispõe o artigo 1º da Constituição Federal, a "*República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito*" e tem como fundamento os valores sociais do trabalho e da livre iniciativa, juntamente com a soberania, cidadania, dignidade da pessoa humana e pluralismo político. Da mesma forma prevê o artigo 5º da Constituição Federal ao tratar dos direitos e deveres individuais e coletivos dos indivíduos, ao inserir o inciso XIII no rol dos direitos fundamentais, garantindo assim o "livre exercício de qualquer trabalho, ofício ou profissão, atendidas as qualificações profissionais que a lei estabelecer"[14].

No entanto, em que pese a livre iniciativa ser extremamente importante para o desenvolvimento de novos negócios, bem como ser importante para a manutenção da ordem econômica, a qual, segundo o artigo 170 da Constituição Federal, tem "*por fim assegurar a todos a existência digna, conforme os ditames da justiça social, observados os princípios da livre concorrência, defesa do consumidor, busca do pleno*

14. BRASIL. Constituição Federal, Art. 5. XIII.

emprego"[15], dentre outros, pode ser que existam limitações ao exercício de determinas atividades, sem configurar um abuso aos dispositivos constitucionais que liberam o indivíduo para o exercício de atividades.

Isso porque, "*é assegurado a todos o livre exercício de qualquer atividade econômica, independentemente de autorização de órgãos públicos, salvo nos casos previstos em lei*"[16]. Portanto, se houver previsão em lei dispondo sobre a necessidade de autorização para o exercício de determinada atividade pelo órgão público competente, o seu exercício não se dará de forma desamarrada, pois dependerá das exigências previstas na lei.

É exatamente essa parte do dispositivo constitucional que dá legitimidade à intervenção estatal, na forma da regulação, para impor a barreira de acesso ao mercado por de ato público de liberação, o qual pode se dar de diversas formas, pois:

> Art. 1º. (...) § 6º (...) , consideram-se atos públicos de liberação a licença, a autorização, a concessão, a inscrição, a permissão, o alvará, o cadastro, o credenciamento, o estudo, o plano, o registro e os demais atos exigidos, sob qualquer denominação, por órgão ou entidade da administração pública na aplicação de legislação, como condição para o exercício de atividade econômica, inclusive o início, a continuação e o fim para a instalação, a construção, a operação, a produção, o funcionamento, o uso, o exercício ou a realização, no âmbito público ou privado, de atividade, serviço, estabelecimento, profissão, instalação, operação, produto, equipamento, veículo, edificação e outros.[17]

Como pode ser observado, a moldura legislativa que trata da limitação da livre iniciativa no exercício de atividade encontra justificativa também na Lei de Liberdade Econômica, qual seja, a Lei n. 13.874, de 20 de setembro de 2019, a qual institui a Declaração de Direitos de Liberdade Econômica e estabelece normas de proteção à livre iniciativa e ao livre exercício de atividade econômica e disposições sobre a atuação do Estado como agente normativo e regulador.

Segundo a Lei, as atividades consideradas de risco moderado ou alto devem ser limitadas, sendo necessário, portanto, ato público de liberação de atividade

15. BRASIL. Constituição Federal. Art. 170.
16. BRASIL. Constituição Federal. Art. 170, p. único.
17. BRASIL. Lei 13.874, de 20 de setembro de 2019. Art 1º, *§ 6º*

econômica para o risco médio (moderado) ou alto. Isso porque, a dispensa de ato público de liberação é apenas para as atividades econômicas de baixo risco. Neste sentido, veja-se:

> Art. 3º São direitos de toda pessoa, natural ou jurídica, essenciais para o desenvolvimento e o crescimento econômicos do País, observado o disposto no parágrafo único do art. 170 da Constituição Federal:
>
> I - Desenvolver atividade econômica de baixo risco, para a qual se valha exclusivamente de propriedade privada própria ou de terceiros consensuais, sem a necessidade de quaisquer atos públicos de liberação da atividade econômica;
>
> (...) § 1º Para fins do disposto no inciso I do caput deste artigo:
>
> I - ato do Poder Executivo federal disporá sobre a classificação de atividades de baixo risco a ser observada na ausência de legislação estadual, distrital ou municipal específica;(...).[18]

Seguindo essa lógica, sobreveio o Decreto n. 10.178 de 2019 com o fim de dispor sobre os critérios e os procedimentos para a classificação de risco de atividade econômica, estabelecendo que:

> Art. 3º O órgão ou a entidade responsável pela decisão administrativa acerca do ato público de liberação classificará o risco da atividade econômica em:
>
> I - nível de risco I - para os casos de risco leve, irrelevante ou inexistente;
>
> II - nível de risco II - para os casos de risco moderado; ou
>
> III - nível de risco III - para os casos de risco alto.
>
> § 1º Ato normativo da autoridade máxima do órgão ou da entidade especificará, de modo exaustivo, as hipóteses de classificação na forma do disposto no caput.
>
> § 2º O órgão ou a entidade poderão enquadrar a atividade econômica em níveis distintos de risco
>
> I - em razão da complexidade, da dimensão ou de outras características e se houver possibilidade de aumento do risco envolvido; ou
>
> II - quando a atividade constituir objeto de dois ou mais atos públicos de liberação,

18. BRASIL. Lei 13.874, de 20 de setembro de 2019. Art. 3º.

> hipótese em que o enquadramento do risco da atividade será realizado por ato público de liberação.
>
> Art. 4º O órgão ou a entidade, para aferir o nível de risco da atividade econômica, considerará, no mínimo:
>
> I - a probabilidade de ocorrência de eventos danosos; e
>
> II - a extensão, a gravidade ou o grau de irreparabilidade do impacto causado à sociedade na hipótese de ocorrência de evento danoso.
>
> Parágrafo único. A classificação do risco será aferida preferencialmente por meio de análise quantitativa e estatística. (...)
>
> Art. 8º O exercício de atividades econômicas enquadradas no nível de risco I dispensa a solicitação de qualquer ato público de liberação.[19]

A conclusão a que se chega é que para a existência de uma de exigência de registro prévio ou qualquer outra modalidade de ato público de liberação do profissional de tecnologia e sistemas, seria necessário:

a) Análise de impacto regulatório sobre o assunto, haja vista que as propostas envolvendo atos normativos de

> "interesse geral de agentes econômicos ou de usuários dos serviços prestados, editadas por órgão ou entidade da administração pública federal, incluídas as autarquias e as fundações públicas, serão precedidas da realização de análise de impacto regulatório, que conterá informações e dados sobre os possíveis efeitos do ato normativo para verificar a razoabilidade do seu impacto econômico."[20];

b) Lei criando órgão regulador específico, com atribuição da competência para regular e disciplinar os serviços relacionados, juntamente com a exigência do ato público de liberação da atividade, conforme determinado o parágrafo único do artigo 170 da Constituição Federal;

c) Classificação do risco da atividade como moderado ou alto, via Portaria do órgão regulador ou outro ato administrativo, para fins de cumprimento do artigo 3º da Lei de Liberdade Econômica.

19. BRASIL. Decreto n. 10.178, de 18 de dezembro de 2019

20. BRASIL. Lei n. 13.874, de 20 de setembro de 2019. Art. 40.

Assim, apesar de a Lei de Liberdade Econômica reforçar a possibilidade de limitação ao exercício de atividades, é correta a afirmação de que isso não será feito de forma desorganizada ou infundada, conforme a escolha do legislador ou até mesmo eventual vontade política oriunda da Administração Pública. Antes, deverá ser averiguado o risco da atividade para a população e para os consumidores da prestação de serviços envolvendo a tecnologia da informação e demais áreas correlatas, sob a justificativa de que a proteção de determinados interesses públicos é superior à essa livre inciativa, tudo documentado em análise de impacto regulatório.

E deve ser ressaltado: a eventual regulação desses profissionais com exigência de registro prévio é via de mão dupla, pois ao mesmo tempo que pode ocasionar consequências pesadas ao desenvolvimento de novos modelos de negócio baseados na internet e conexão de dispositivos, pode favorecer a organização e valorização da profissão frente ao cumprimento de deveres e regras de conduta, conforme se verá adiante.

4. PONTOS POSITIVOS E NEGATIVOS DA REGULAÇÃO SOBRE AS ATIVIDADES ENVOLVENDO TECNOLOGIA E SISTEMAS COM EXIGÊNCIA DE REGISTRO PRÉVIO

Neste tópico será feita uma balança comparativa entre os pontos positivos e negativos de uma eventual regulação específica das atividades envolvendo a prestação de serviços de tecnologia e sistemas, mas sem o intuito de exaurir todas as possibilidades.

Um dos benefícios que a existência do registro prévio poderia trazer é a maior segurança jurídica ao consumidor do serviço, haja vista que a Lei n. 8.078/90 conceitua como consumidor toda pessoa física ou jurídica que adquira ou utilize produto ou serviço como destinatário final[21], e como fornecedor[22] a pessoa física ou jurídica que desenvolva atividade econômica voltada à distribuição de produtos[23] ou

21. BRASIL. Lei n. 8.078/90. 11 de setembro de 1990. Art. 2º.

22. BRASIL. Lei n. 8.078/90. 11 de setembro de 1990. Art. 3º.

23. BRASIL. Lei n. 8.078/90. 11 de setembro de 1990. *Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação,*

prestação serviços[24], o que dá o direito ao consumidor de ter acesso à informação[25] adequada, clara, precisa e ostensiva[26] sobre as suas características, inclusive sobre os riscos que apresentam. Com o registro prévio do profissional, o consumidor poderia verificar se o sujeito que fornece os serviços de fato está qualificado para o exercício das atividades, haja vista o conhecimento técnico necessário para tanto.

Se o registro prévio ou outro ato público de liberação exigir também certificações ou programa de educação continuada para manutenção da atividade, certamente o profissional iria se beneficiar com a qualidade na prestação de seus serviços, bem como o consumidor pela expectativa que o serviço seria prestado por um profissional atualizado e com a *expertise* necessária para tanto.

Um outro ponto positivo seria o cumprimento de deveres legais impostos pela regulação, como por exemplo regras de conduta e vedações. Como exemplo, cita-se a regra de exercer as atividades com boa-fé é ética empresarial, sendo vedada a utilização, por exemplo, de programação para o uso de atividades ilícitas, como: lavagem de dinheiro; a manipulação errônea de exames de saúde; a desregulação de bombas de combustíveis, dentre vários outros pontos que poderiam afetar toda a sociedade em razão do impacto que um programa ou *software* pode ter em um determinado mercado, empresa, negócio e até no dia a dia das pessoas.

Adentrando-se nos pontos negativos da eventual exigência de registro prévio para o exercício profissional das atividades envolvendo tecnologia e sistemas, tem-se o surgimento de um mercado marginal daqueles que não obtiveram o devido registro, o que ocorreria pela simples leitura da Lei de contravenções penais e a infração de

---

exportação, distribuição ou comercialização de produtos ou prestação de serviços. § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.

24. BRASIL. Lei n. 8.078/90. 11 de setembro de 1990. *Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços. (...) § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.*
25. BRASIL. Lei n. 8.078/90. 11 de setembro de 1990. Art. 6º, III.
26. BRASIL. Lei n. 8.078/90. 11 de setembro de 1990. Art. 31.

exercício irregular de profissão:

> CAPÍTULO VI - DAS CONTRAVENÇÕES RELATIVAS À ORGANIZAÇÃO DO TRABALHO
>
> Art. 47. Exercer profissão ou atividade econômica ou anunciar que a exerce, sem preencher as condições a que por lei está subordinado o seu exercício:
>
> Pena – prisão simples, de quinze dias a três meses, ou multa, de quinhentos mil réis a cinco contos de réis.[27]

Sem qualquer intuito de verificar os contornos do tipo penal e análise dos elementos subjetivo e objetivo do artigo, é certo que a exigência de um registro iria tornar grande parte dos negócios envolvendo essa prestação de serviços algo irregular, o que pode ser considerado um ponto negativo, pois envolve custos e despesas à Administração Pública.

Um outro ponto negativo seria o da responsabilidade pela fiscalização dos registros dentro das empresas: seria necessária a criação de um *compliance*, com diretor estatutário, para verificar quem tem (e quem não tem) o devido registro? Como isso seria feito? Neste ponto, o custo poderia aumentar para a iniciativa privada, a qual teria que pagar inclusive a taxa de fiscalização em razão do exercício do poder de polícia[28] para o órgão regulador competente, além de outras contribuições para

27. BRASIL. Decreto-lei n. 3.688, de 3 de outubro de 1941. Art. 47.

28. BRASIL. Lei n. 5.172, de 25 de outubro de 1966. *Art. 77. As taxas cobradas pela União, pelos Estados, pelo Distrito Federal ou pelos Municípios, no âmbito de suas respectivas atribuições, têm como fato gerador o exercício regular do poder de polícia, ou a utilização, efetiva ou potencial, de serviço público específico e divisível, prestado ao contribuinte ou posto à sua disposição. Parágrafo único. A taxa não pode ter base de cálculo ou fato gerador idênticos aos que correspondam a imposto nem ser calculada em função do capital das empresas. Art. 78. Considera-se poder de polícia atividade da administração pública que, limitando ou disciplinando direito, interesse ou liberdade, regula a prática de ato ou abstenção de fato, em razão de interesse público concernente à segurança, à higiene, à ordem, aos costumes, à disciplina da produção e do mercado, ao exercício de atividades econômicas dependentes de concessão ou autorização do Poder Público, à tranquilidade pública ou ao respeito à propriedade e aos direitos individuais ou coletivos. Parágrafo único. Considera-se regular o exercício do poder de polícia quando desempenhado pelo órgão competente nos limites da lei aplicável, com observância do processo legal e, tratando-se de atividade que a lei tenha como discricionária, sem abuso ou desvio de poder.*

eventual instituição autorreguladora e custos com certificações impostas pelos atos administrativos normativos.

Em suma, o custo da exigência pode ser grande, apresentando impactos nas diversas searas do direito, como é o caso do direito penal e direito do consumidor, o que deve ser levado em consideração em uma análise mais ampla da necessidade de ato público de liberação.

5. CONCLUSÃO

De um lado, o sujeito é livre para empreender e ser contratado. De outro, a regulação pode impor limites à essa liberdade, com exigência de registro prévio para a regularidade da atividade, sob pena de o sujeito cometer uma infração em âmbito penal, haja vista o dispositivo na Lei das Contravenções penais, que proíbe o exercício de profissão ou atividade econômica sem preencher as condições impostas pela lei.

Para o caso apresentado, qual seja, o mercado onde se inserem os profissionais de tecnologia e sistemas, como os programadores e desenvolvedores, analistas de tecnologia da informação, dentre outros, não foi verificada a existência de uma regulação específica para o profissional, mesmo com a existência de decretos dispondo sobre os objetivos das estratégias governamentais para desenvolvimento e fomento da chamada "economia digital".

Nesse sentido, afirmar que o princípio da livre iniciativa deve se sobrepor a quaisquer atuações Estatais que limitam o exercício de atividades econômicas não é correto. Em verdade, uma das funções do Estado regulador é exatamente essa, impor limites às vontades negociais dos indivíduos para proteger interesses maiores, com o fim de proteger o próprio mercado e garantir o bem estar da população e ordem econômica.

Essa reflexão, entretanto, não sugere que a atividade do Estado se dê de forma infundada e desorganizada, sendo necessário, em primeiro lugar, estudar o impacto de qualquer mudança regulatória no mercado analisado.

Assim, para exigir o registro prévio desses profissionais, ou exigir qualquer ato público de liberação, não há outro caminho a não ser a criação de uma lei especial

nesse sentido, estabelecendo, dentre as diversas regras de conduta típicas da regulação de atividades econômicas classificadas como moderada ou alta, que o exercício profissional daquela atividade somente possa ser exercido por aquele que se registrou conforme determina a lei.

Desta forma, a hipótese formulada de que a existência de registro prévio para o desenvolvimento das atividades mencionadas não fere os princípios da livre iniciativa é confirmada, mas desde que haja uma lei específica dispondo sobre essa possibilidade e o cumprimento de outros requisitos legais, conforme apresentado neste artigo.

REFERÊNCIAS

BONFADINI, Paulo André Espírito Santo. *O poder normativo autônomo das agências reguladoras*. Critérios e controles. Rio de Janeiro: Lumen Juris, 2021.

BRASIL. Congresso Nacional. *Constituição da República Federativa do Brasil, de 5 de outubro de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 ago. 202

BRASIL. Congresso Nacional. Lei n. 13.874, de 20 de setembro de 2019. *Institui a Declaração de Direitos de Liberdade Econômica; estabelece garantias de livre mercado; altera as Leis nos 10.406, de 10 de janeiro de 2002 (Código Civil), 6.404, de 15 de dezembro de 1976, 11.598, de 3 de dezembro de 2007, 12.682, de 9 de julho de 2012, 6.015, de 31 de dezembro de 1973, 10.522, de 19 de julho de 2002, 8.934, de 18 de novembro 1994, o Decreto-Lei nº 9.760, de 5 de setembro de 1946 e a Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943; revoga a Lei Delegada nº 4, de 26 de setembro de 1962, a Lei nº 11.887, de 24 de dezembro de 2008, e dispositivos do Decreto-Lei nº 73, de 21 de novembro de 1966; e dá outras providências*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm> Acesso em: 25 ago. 2021.

BRASIL. Congresso Nacional. Lei n. 5.172, de 25 de outubro de 1966. Código Tributário Nacional. *Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm>. Acesso em: 28 fev. 2022.

BRASIL. Congresso Nacional. Lei n. 8.078, de 11 de setembro de 1990. *Dispõe sobre a proteção do consumidor e dá outras providências.* Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 25 ago. 2021.

BRASIL. Decreto-lei n. 3.688, de 3 de outubro de 1941. *Lei das Contravenções Penais*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3688.htm> Acesso em: 25 ago. 2021.

BRASIL. Presidência da República. *Decreto n. 10.178, de 18 de dezembro de 2019. Regulamenta dispositivos da Lei nº 13.874, de 20 de setembro de 2019, para dispor sobre os critérios e os procedimentos para a classificação de risco de atividade econômica e para fixar o prazo para aprovação tácita e altera o Decreto nº 9.094, de 17 de julho de 2017, para incluir elementos na Carta de Serviços ao Usuário*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10178.htm> Acesso em: 25 ago. 2021.

BRASIL. Presidência da República. Decreto n. 9.319, de 21 de março de 2018. *Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm>.Acesso em: 25 ago. 2021.

BRASIL. Presidência da República. *Decreto n. 9.854, de 25 de junho de 2019. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas*. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm>. Acesso em: 25 ago. 2021.

REZENDE, Denis Alcides. Evolução da Tecnologia da Informação nos últimos 45 anos. *Revista FAE Business*, v. 4, p. 42-46, 2002

SANTOS, Ester Laodiceia Santos. *O profissional da informação em atividades de inteligência competitiva*. Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Escola de Ciência da Informação da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Mestre em Ciência da Informação. Belo Horizonte, 2009.

SOUZA, Élida Patrícia de. *Carreira em tecnologia da informação*: um estudo junto a profissionais de Minas Gerais. Tese apresentada ao Centro de Pós Graduação e Pesquisas em Administração da Universidade Federal de Minas Gerais, como requisito parcial para a obtenção do título de Doutorado em Administração. Belo Horizonte, 2018";

SANTOS, Bruno P. SILVA, Lucas A. M; CELES, Clayson S. F. S; NETO, João B. Borges; PERES, Bruna S; VIEIRA, Marcos Augusto M.; Vieira, Luiz Filipe M.; Goussevskaia Olga N; LOUREIRO, Antônio A. F. *Internet das Coisas*: da Teoria à Prática. Departamento de Ciência da Computação Universidade Federal de Minas Gerais (UFMG) Belo Horizonte, 2019.

INVESTIGAÇÃO CIVIL SOBRE ILÍCITOS INFORMÁTICOS

Gabriel Franco Jallais
Graduando em Ciência da Computação pela Universidade Federal de Minas Gerais.

Giovanni Carlo Batista Ferrari
Graduado em Direito na Universidade Federal de Minas Gerais. Pós-graduado em Direito Digital e Direito do Consumidor. Advogado.

DOI: https://doi.org/10.59224/dti5.ch6

Resumo: Este artigo mostra como os ataques cibernéticos e crimes praticados através da internet estão crescendo no Brasil, e como um civil pode realizar a investigação para alcançar quem lhe causou um dano. Foram descritos meios técnicos e jurídicos para a identificação dos atacantes, bem como as maneiras que eles utilizam para dissimular seus atos. Então chega-se à conclusão que é viável a investigação, desde que o atacante não utilize meios evasivos acerca de sua identidade real.

Palavras-chave: investigação civil; internet das coisas; ilícitos.

Abstract: *In the article we analyze how cyber attacks and crimes committed through the internet are growing in Brazil, and how a civilian can carry out the investigation to reach who caused him harm. Technical and legal means to identify attackers were described, as well as the ways they use to conceal their actions. Then, the conclusion is reached that the investigation is viable, as long as the attacker does not use evasive means about his real identity.*

Keywords: *civil investigations; Internet of Things; torts.*

---

anonimização na internet; 4.2. IoT do lado do atacante; 4.3. Identificando o verdadeiro IP; 4.4. Viabilidade da continuidade da investigação nesses casos; 5. Reparação das perdas e danos da vítima; 6. Conclusão; Referências.

1. INTRODUÇÃO: A VIABILIDADE JURÍDICA DE UMA INVESTIGAÇÃO PRIVADA

No Brasil, há a possibilidade de um cidadão poder investigar por si próprio, algum ato ilícito de que ele tenha sido vítima, através do meio informático.

Nesse sentido, desde a publicação da lei federal n° 12.965/2014, mais conhecida como Marco Civil da Internet (MCI), o cidadão pode, através de dispositivos jurídicos específicos, ter a capacidade de acionar um advogado e uma empresa especializada em investigação, e com recursos próprios desenvolver uma investigação para encontrar o possível perpetrador do ato ilícito que ele tenha sido vítima.

Tal situação de investigação privada acontece por conta da ineficiência dos órgãos estatais em combater esse tipo de crime, seja por falta de equipamentos ou de pessoal especializado nessa incumbência. Esse contexto de pouca investigação e impunidade faz com que os criminosos tenham um incentivo para praticar esse tipo de delito.

Além disso, nos últimos anos, a exemplo do relato do investigador de polícia Michel Weiler Neves[1], especialista em crimes cibernéticos da Secretaria de Segurança Pública do Estado do Mato Grosso do Sul, os crimes cibernéticos registrados naquele estado quase dobraram, pois os registros passaram de 1.781 em 2020, para 3.529 em 2021. Nesse sentido, o Ministério Público do Estado de Minas Gerais publicou[2] que no ano de 2021, foram registrados 32.949 casos envolvendo fraudes *online* naquele

1. Disponível em: http://www.ms.gov.br/crimes-virtuais-policia-de-ms-registrou-mais-de-35-mil-ocorrencias-em-2021-neste-ano-ja-sao-1-126-casos/#:~:text=Em%20Mato%20Grosso%20do%20Sul,j%C3%A1%20foram%20registrados%201.126%20casos. Acesso em 22 de junho de 2022.
2. Disponível em: https://www.mpmg.mp.br/portal/menu/comunicacao/noticias/estelionato-digital-mpmg-intensifica-atuacao-para-combater-golpes-pelowhatsappem-mg-8A9480687CEBDB46017CF0ECEB305789-00.shtml#:~:text=Em%20Minas%20Gerais%2C%20conforme%20levantamento,aplicado%20pelo%20aplicativo%20no%20estado. Acesso em 22 de junho de 2022.

estado.

Assim sendo, caso uma vítima queira mitigar suas próprias perdas e identificar rapidamente o autor do prejuízo que sofreu, a investigação privada é uma alternativa viável.

No contexto dos ataques cibernéticos, outra situação vem ganhando notoriedade, o ataque a dispositivos de internet das coisas (IoT). Por tais dispositivos serem tantos e tão diversos, em fabricantes e tecnologias envolvidas, torna-se um desafio realizar a investigação nesses objetos a fim de identificar a fonte de ataque.

Nesse contexto, o objetivo do presente artigo é demonstrar a trajetória de uma investigação diante de ataques cibernéticos virtuais que causaram prejuízos à vítima, bem como identificar e contornar os meios furtivos que eles eventualmente utilizaram.

Serão considerados apenas casos em que o atacante é pouco habilidoso, isto é, não utiliza de artifícios demasiadamente complexos tanto para invadir o aparelho quanto para ocultar seus rastros, visto que, nesses casos, é extremamente difícil ou até inviável chegar ao atacante por meio de uma investigação privada. Ademais, consideramos ataques via rede de internet da vítima, visto que este será o protocolo mais comum dentre os dispositivos IoT.

2. ATAQUES VIA INTERNET EM DISPOSITIVOS IOT

Um ataque virtual é uma iniciativa mal-intencionada e deliberada, perpetrado por um indivíduo ou empresa, direcionados a redes ou sistemas para aquisição de dados e causar danos.

Nesse diapasão, será feita uma análise mais detalhada sobre como se operam os ataques virtuais em dispositivos conectados à internet, destacando as principais vulnerabilidades desses sistemas, bem como a dificuldade jurídica em identificar quem de fato são os atacantes.

Não abordaremos aqui ataques executados diretamente sobre o hardware desses equipamentos, pois fugiria do tema e tornaria este trabalho mais extenso.

2.1. VULNERABILIDADE DOS EQUIPAMENTOS DE IOT

Todo e qualquer sistema eletrônico possui falhas, o que difere os equipamentos IoT dos demais, é a integração entre diversos dispositivos heterogêneos, através de diferentes protocolos de comunicação, o que abre mais possibilidade para ataques e propagação de falhas.

Nesse sentido, pode-se visualizar as vulnerabilidades presentes nos aparelhos IoT por meio de três superfícies de ataque[3], sendo elas, a camada de interface de protocolo, a camada de *hardware*, e por fim, a camada de *software*, estas superfícies estão presentes em outros cenários da cibersegurança, não só nos sistemas IoT.

2.1.1. CAMADA DE INTERFACE DE PROTOCOLO

A camada de interface de protocolo engloba as possíveis falhas na comunicação e na interface de programação de aplicação (API[4]), envolvendo tanto os equipamentos utilizados pelo usuário quanto a *cloud*[5] com a qual esses dispositivos mantêm contato.

Nela, são três os principais fatores que abrem espaço para falhas: interfaces inseguras de gerenciamento remoto, vazamento de informações sensíveis durante a transmissão de dados e autenticação fraca. O primeiro, permite ataques como *SQL*

3. Segundo a empresa de cibersegurança Fortinet, a superfície de ataque é o número de todos os possíveis pontos, ou vetores de ataque, nos quais um usuário não autorizado obtém acesso ao sistema e extrai dados. Disponível em https://www.fortinet.com/resources/cyberglossary/attack-surface. Acesso em 28 de junho de 2022.
4. De acordo com a empresa Amazon, APIs são mecanismos que permitem que dois componentes de software se comuniquem usando um conjunto de definições e protocolos. Disponível em https://aws.amazon.com/pt/what-is/api/#:~:text=API%20significa%20Application%20Programming%20Interface,de%20servi%C3%A7o%20entre%20duas%20aplica%C3%A7%C3%B5es. Acesso em 28 de junho de 2022.
5. Segundo a empresa de software IBM, a cloud computing "*é o acesso sob demanda, via internet, a recursos de computação — aplicativos, servidores (físicos e virtuais), armazenamento de dados, ferramentas de desenvolvimento, recursos de rede e muito mais — hospedados em um data center remoto gerenciado por um provedor de serviços em cloud (ou CSP). O CSP disponibiliza esses recursos por uma assinatura mensal ou por um valor cobrado conforme o uso".* Disponível em https://www.ibm.com/br-pt/cloud/learn/cloud-computing. Acesso em 28 de junho de 2022.

injection, *Cross-site Scripting (XSS)* e execução remota de programas. Já o segundo, ocorre quando o aparelho não utiliza de bons algoritmos de encriptação para ocultar os dados transmitidos. Por fim, o terceiro se dá em função do fato que os dispositivos IoT requerem autenticação uns dos outros para validar a conexão e a comunicação entre si, contudo, quando ela é facilmente contornável, usuários e dispositivos não autorizados podem obter acesso à rede de equipamentos e a dados sensíveis.

2.1.2. CAMADA DE *HARDWARE*

Na camada de *hardware*, de maneira semelhante a anterior, podem ser identificados três aspectos principais que concedem abertura para ataques, sendo eles, interface de depuração não segura, memória flash desprotegida e vazamento de informação sensível do hardware, como chaves de encriptação. Os dois primeiros são especialmente sensíveis pois permitem que o atacante tenha acesso ao *firmware* do dispositivo, seja para analisá-lo e elaborar formas de contornar a autenticação, modificá-lo ou até substituí-lo.

Firmware é um conjunto de instruções fundamentais de um *hardware*, que especificam como ele deve se comunicar com as outras partes que o compõe e com outros aparelhos, além de como realizar tarefas básicas do sistema.

2.1.3. CAMADA DE *SOFTWARE*

Já na camada de *software*, mais fatores estão presentes, como os equipamentos IoT, geralmente, possuem hardware de pequeno porte, a parte do software prevalece quando se trata de complexidade e vulnerabilidade, visto que esta é responsável por processar a comunicação, gerar requisitos para outros dispositivos, gerar dados, processar dados e muito mais, é o que permite a integração entre os dispositivos. As principais falhas e mais críticas são: *bootloader* vulnerável, sistema operacional vulnerável, vazamento de dados sensíveis no *firmware*, serviço de aplicação vulnerável e estratégias ruins de configuração, como senhas fracas ou autenticação pouco robusta por padrão.

O *bootloader* é o programa responsável pela inicialização do sistema e do *firmware*, se ele possui alguma falha, um atacante consegue facilmente obter acesso ao

sistema. Um caso famoso envolvendo falhas no *bootloader* foi o *checkm8*[6], uma exploração na ROM (*Read Only Memory*) que armazena instruções de *boot* nos dispositivos da Apple.

Em suma, as falhas presentes na camada de *software* se dão devido a um mal desenvolvimento do programa, seja por falta de revisão dos códigos ou estratégia, bem como pressa para a disponibilização do produto, elas também podem ocorrer em função dos recursos limitados nos equipamentos IoT, o que prejudica a implementação de barreiras de segurança e robustez. Os problemas encontrados no sistema operacional e o vazamento de dados ocorrem justamente em consequência desse fator, com pouco espaço de armazenamento, o *kernel* do sistema operacional é limitado, além disso, muitas vezes não está na versão mais recente, o que acarreta em múltiplos outros problemas. Em adição a isso, o pouco espaço de armazenamento traz mais um desafio, não na questão da vulnerabilidade a ataques, mas sim na volatilidade dos dados armazenados, devido ao tamanho, as informações contidas nelas são reescritas constantemente por dados mais recentes, o que pode acabar destruindo evidências para uma investigação.

2.1.4. O USUÁRIO COMO VULNERABILIDADE

Ademais, a vulnerabilidade mais comum na esfera da IoT e de dispositivos eletrônicos como um todo, é o próprio usuário, que concede acesso a criminosos em função do mal uso do dispositivo ou por meio de engenharia social.

No contexto socioeconômico e educacional brasileiro, a desinformação por grande parte da população em relação ao uso de equipamentos eletrônicos é uma excelente ferramenta para cibercriminosos.

Não cabe no escopo deste trabalho discutir as minúcias de cada possível falha encontrada nos dispositivos IoT, em especial as presentes no *hardware*, como dito anteriormente, tampouco de cada superfície de ataque, por essa razão foram apenas expostas as vulnerabilidades mais comuns presentes nestes aparatos para uma visão geral do cenário no qual o ataque efetuado contra o civil possa ter ocorrido.

6. Disponível em:< https://checkm8.info/ > e <https://periciacomputacional.com/tudo-o-que-voce-sempre-quis-perguntar-sobre-o-checkm8-e-o-checkra1n/>. Acessos em 29 de junho de 2022.

2.2. DIFICULDADES JURÍDICAS DA INVESTIGAÇÃO

Como os dispositivos informáticos e de IoT são diversos, envolvendo tecnologias e desenvolvedores diferentes, durante a investigação, o investigador pode se deparar com um atacante oriundo de outro país, necessitando, assim, de cooperação internacional, a fim de serem respeitadas a soberania e jurisdição do outro Estado.

O conceito de soberania, segundo José Cretella Júnior, é que "a soberania é, realmente, fundamento do Estado, qualquer que seja sua forma, monárquica ou republicana, federativa ou unitária, porque o Estado 'é síntese dos poderes soberanos'. Soberania é a situação do Estado que não está submetido a outro e que, por isso, pode elaborar sua Constituição, ou seja, pode criar seu direito positivo no mais alto grau.[7]"

Já o conceito de jurisdição, nos ensinamentos de Freddie Didier Júnior é "a função atribuída a terceiro imparcial, de realizar o direito de modo imperativo e criativo, reconhecendo/protegendo/efetivando situações jurídicas concretamente deduzidas, em decisão insuscetível de controle externo, e com aptidão para torna-se indiscutível".[8]

Assim sendo, conforme argumentado por Oriwoh[9], há dificuldade em identificar os suspeitos do ataque cibernético devido à variedade de leis e jurisdições distintas, pois os atacantes e os dados necessários para elucidar o crime podem estar regidos por normas que o investigador pouco compreende.

Tendo em vista essa situação, em 2001, na Hungria, foi realizada a Convenção de Budapeste sobre o Cibercrime, que trata sobre a criminalização de condutas, orienta a criação de normas para investigação e produção de provas eletrônicas, e meios de cooperação internacional são questões tratadas neste documento. Ele ainda aborda a questão do acesso indevido e não autorizado a sistemas de computador, fraudes, material de pedofilia, violações de direitos autorais e violações de segurança de redes. O Senado Federal aprovou a adesão do Brasil a esta convenção desde 15 de dezembro

7. CRETELLA JÚNIOR, José. *Comentários à Constituição brasileira de 1988*. 3. ed. Rio de Janeiro : Forense Universitária, v. 1, 1992.
8. DIDIER JR, Fredie. *Curso de direito processual civil*. Juspodium: Salvador, 11ª Ed., p. 83. 2008.
9. ORIWOH, Ewede. Disponível em https://www.researchgate.net/publication/258093766_Internet_of_Things_Forensics_Challenges_and_Approaches . Acesso em 28 de junho de 2022.

de 2021, o que trará mais ferramentas para que uma investigação seja frutífera em adquirir dados sobre um crime virtual e possibilitar a identificação dos suspeitos.

3. O PASSO-A-PASSO DA INVESTIGAÇÃO CIBERNÉTICA

A investigação cibernética deve ser feita levando em consideração os direitos do investigado, em especial de sua privacidade. Nesse sentido, os provedores de aplicação e de conexão da internet são fontes importantíssimas para se encontrar o autor de um crime cometido pelo meio informático, e lá também se encontram informações relacionadas à privacidade do indivíduo, que, se não forem relacionadas ao crime, não podem ser devassadas e usadas contra ele.

A privacidade do brasileiro é garantida pelo art. 5°, X da Constituição da República: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação." Dessa forma, o texto constitucional deixa clara a importância desse instituto na vida de uma pessoa.

Nessa ótica, o MCI deixa claro em seus dispositivos a necessidade da preservação da privacidade do usuário de internet, bem como o sigilo sobre seus dados[10]. Assim sendo, para que alguém consiga os dados de acesso das aplicações e dos provedores de conexão, é necessário que haja autorização judicial para tanto, para fins de preservação dos direitos da personalidade do usuário sob suspeita de práticas ilícitas.

O art. 22[11] do MCI deixa claro que o interessado, a fim de constituir provas para

10. "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
(...)
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

11. "Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo

um processo cível ou criminal, pode requerer ao juiz que ordene aos provedores de aplicação e conexão que forneçam os dados de acesso necessários. Assim, a parte interessada deve demonstrar em juízo a prática do ilícito do qual foi vítima, a utilidade daqueles dados para fins investigatórios e especificando ainda o período de tempo sobre os registros.

Dessa forma, é possível realizar o procedimento investigatório privado, para fins de identificar os malfeitores e requerer a reparação em perdas e danos dos prejuízos sofridos.

3.1. REQUISIÇÃO DE ACESSO AO PROVEDOR DE APLICAÇÃO

Quando uma pessoa sofre um ataque cibernético em seu computador ou dispositivo IoT, esse ataque deixa vestígios nos registros do sistema, bem como a conexão por endereço *Internet Protocol* (IP)[12] que ele fez com o software ou dispositivo da vítima. Dessa forma, a vítima precisa desse número para identificar o atacante e sua localização.

Conforme determina o art. 15 do MCI[13], o provedor de aplicações é obrigado a

---

judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros."

12. Segundo a empresa de segurança Kaspersky, "*o endereço IP é um endereço exclusivo que identifica um dispositivo na Internet ou em uma rede local. O IP consiste em um conjunto de regras que regem o formato de dados enviados pela Internet ou por uma rede local. Basicamente, o endereço IP é o identificador que permite que as informações sejam enviadas entre dispositivos em uma rede: ele contém as informações de localização e torna o dispositivo acessível para comunicação*". Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address . Acesso em 23 de junho de 2022.
13. "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os

guardar os registros de acesso pelo prazo de 6 meses. Dessa forma, para acessar esses dados, é necessária ordem judicial específica, conforme art. 10 do MCI[14]. Nesse sentido, a vítima deve recorrer a um juiz e requerer o acesso aos dados daquele atacante, em especial o IP referente à conexão que ele utilizou, em determinado espaço de tempo.

Uma vez deferido ao autor o pedido judicial, ele deverá identificar qual é a origem e qual o provedor de conexão daquele IP, naquela hora específica. O MCI determina ainda que o provedor de aplicações é obrigado a guardar os dados de acesso por seis meses, tal prazo possibilita o acesso da vítima aos dados do atacante, de forma que ela tenha tempo para tomar todas as medidas legais e técnicas cabíveis para investigar a dinâmica de como o ataque aconteceu.

3.2. IDENTIFICANDO O PROVEDOR DE CONEXÃO

Em posse do endereço de IP utilizado pelo criminoso é possível consultar qual é o provedor de internet que detém este endereço por meio de ferramentas como a *whois*, disponíveis em sites de organizações responsáveis por supervisionar e registrar endereços e domínios da internet, sendo a principal delas a IANA (Autoridade para Atribuição de Números da Internet), a autoridade global responsável por esta tarefa, em âmbito regional encontra-se a *nic.br*, brasileira, e a *LACNIC* (Registro Regional da Internet para a região da América Latina e Caribe). Ao entrar em suas plataformas basta fornecer o número de IP e será retornada um texto no seguinte formato:

---

respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento."

14. "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º".

"*inetnum*: 186.212.0.0/14

asn: AS18881

c-abusos: CSTBR

titular: TELEFÔNICA BRASIL S.A

documento: 02.558.157/0001-62

responsável: Diretoria de Planejamento e Tecnologia

país: BR

c-titular: ARITE

c-técnico: GVO6

inetrev: 186.213.0.0/16

servidor DNS: dns1.gvt.net.br

status DNS: 08/07/2022 AA

último AA: 08/07/2022

servidor DNS: dns2.gvt.net.br

status DNS: 08/07/2022 AA

último AA: 08/07/2022

servidor DNS: dns3.gvt.net.br

status DNS: 08/07/2022 AA

último AA: 08/07/2022

criado: 11/06/2010

alterado: 09/09/2016

Contato (ID): ARITE

nome: Administração Rede IP Telesp

e-mail: dominios-vivo.br@telefonica.com

país: BR

criado: 07/04/2008

alterado: 04/01/2022

Contato (ID): CSTBR

nome: CSIRT TELEFONICA BR

e-mail: abuse.br@telefonica.com

país: BR

criado: 13/07/2018

alterado: 13/07/2018

Contato (ID): GVO6

nome: GVT Operacao

e-mail: c.servicoip.br@telefonica.com

país: BR

criado: 13/06/2001

alterado: 31/03/2022"

No caso, o IP fornecido está sob posse da Telefônica Brasil S.A, a operadora Vivo, em algumas consultas, endereços físicos são fornecidos, estes endereços não se referem ao local de onde o criminoso perpetrou o ataque, mas sim, o endereço comercial ou do servidor do provedor de acesso.

3.3. REQUISIÇÃO DE DADOS DO PROVEDOR DE CONEXÃO

Após a identificação do provedor de conexão à internet, é necessário entrar em contato com esta empresa para adquirir os dados de conexão daquele IP específico, que foi utilizado em uma hora determinada. Nesse contexto, de acordo com o art. 13 do MCI, a lei determina que os registros de conexão sejam guardados por um ano, e também somente podem ser acessados mediante autorização judicial nesse sentido.

Nesse diapasão, o provedor de conexão pode identificar qual é a conta vinculada àquela conexão com a internet, podendo fornecer o nome do consumidor, cadastro de pessoa física da Receita Federal e seu endereço físico. Dessa forma, consegue-se, em regra, chegar num atacante.

Acontece que tal atacante pode estar conectado clandestinamente à rede de

terceiros, seja um vizinho ou empresa, o que pode criar outro obstáculo no momento de identificar o real malfeitor, pois seria necessário identificar as conexões do roteador, endereço MAC, e ou o IMEI[15] de equipamentos utilizados, fazendo análise desses registros.

Assim sendo, observa-se que o direito constitucional dos cidadãos de preservação da privacidade foi respeitado pela norma legal, e o investigador, caso queira acessar tais dados para identificar o criminoso, deverá fazê-lo mediante ação judicial.

3.4. DIFICULDADE EM IDENTIFICAR O EQUIPAMENTO UTILIZADO PELO ATACANTE

Considerando o primeiro cenário, em que o criminoso utiliza a rede da própria residência para realizar o ataque, a solução é simples, após solicitados os dados do assinante do serviço de internet, requer-se a um juiz o acesso aos equipamentos desse e efetua-se uma análise no roteador e demais dispositivos, com fins de confirmar a autoria do crime.

Não obstante, no segundo cenário, caso a rede utilizada para perpetrar o crime seja de um terceiro, a tarefa se torna mais complicada. Umas das formas de se chegar ao verdadeiro dispositivo utilizado, e assim ao autor do crime, é analisar os acessos realizados por meio daquela rede, isto é, os endereços MAC e IMEI dos dispositivos utilizados e o histórico de acesso, que a priori não é rastreado, mas em caso de investigação pode vir a ser, assim, caso o criminoso mantenha sua conexão por meio daquela rede ele poderá ser identificado. Contudo, segundo o art. 14 do MCI, a lei determina que na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet, portanto, sem autorização prévia do assinante do serviço o acesso a esses registros não é possível.

Caso esse terceiro decida por colaborar com a investigação, é possível obter as informações descritas acima e possivelmente chegar ao atacante, no entanto, se ele não utilizar a rede novamente, somente com IMEI ou endereço MAC do dispositivo

15. IMEI significa "*International Mobile Equipment Identity*", que é o número do registro daquele equipamento, para que operadoras e fabricantes de telefones possam identificar aquele aparelho e suas características. O número do IMEI de um celular pode ser visto em seu interior, na nota de compra ou digitando as teclas *#06#.

utilizado dificilmente serão obtidos dados relevantes, já que, em posse do IMEI, se o criminoso receber mensagens ou realizar ligações, ele só poderá ser rastreado pela polícia. Com o endereço MAC as possibilidades são igualmente escassas, dado que, só é possível identificar o fabricante do eletrônico, que muitas vezes terá sede em outro país e, por conseguinte, estará sob outra jurisdição, o que torna a busca inviável para uma investigação privada.

Ainda que fosse viável a busca do equipamento por meio dessas informações, haveria muitos intermediadores de compra e venda para o rastreio através de informações do fabricante, além disso, dentro do contexto brasileiro, há grandes chances de o equipamento ter sido obtido por meio de familiares, pela compra, em dinheiro, com pessoas físicas, como o mercado de usados, ou até através de furto, ou seja, sem registro formal da posse daquele aparelho.

Ademais, no caso de um ambiente público, um aeroporto por exemplo, a investigação se torna ainda mais complexa, devido ao alto tráfego de pessoas todos os dias

Dessa forma, vê-se que identificar o aparelho por meio do qual efetuou-se o crime, na maioria dos casos, será extremamente complicado e provavelmente infrutífero.

3.5. GEOLOCALIZAÇÃO

A geolocalização é a identificação de um dispositivo no espaço geográfico. Tal localização pode ser aproximadamente obtida através da triangulação do sinal das antenas dos aparelhos de telefone celular, pois o aparelho está sempre conectado a uma ou mais antenas para melhor captar o sinal de comunicação. Dessa forma, consegue-se identificar alguém com certa precisão no espaço.

No Brasil, não há regra clara sobre fornecimento de dados de geolocalização de uma pessoa. Tais dados de geolocalização são dados pessoais e por isso devem ser tratados com segurança e sigilo por parte das operadoras de telecomunicações, conforme determina a lei federal nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

Para a vítima de um crime virtual ter acesso a esse tipo de informação de geolocalização do atacante, ele deverá também ter autorização judicial nesse sentido, uma vez que tais dados podem atingir a privacidade do investigado, que também é sujeito

de direito e não pode ter sua intimidade devassada em aspectos alheios à sua conduta criminosa.

O Superior Tribunal de Justiça (STJ), no RMS 68.199/RJ, já manifestou que é possível requerer dados estáticos, registros de geolocalização, relacionados à identificação de usuários que operam em área delimitada, por intervalo de tempo indicado. Tal situação configura quebra de sigilo de dados informáticos estáticos, não configurando interceptação da comunicação. A corte ainda arguiu que não existem direitos constitucionais de caráter absoluto, podendo esses direitos serem relativizados excepcionalmente, por medidas de interesse público, desde que respeitados os termos estabelecidos pela própria Constituição. Como requisito legal, o STJ estabeleceu que devem ser respeitados os seguintes elementos previstos em lei[16]: indícios de ocorrência do ilícito, justificativa da utilidade da requisição e período ao qual se referem os registros.

3.5.1. RASTREAMENTO TÉCNICO DE GEOLOCALIZAÇÃO

No contexto de uma investigação privada, onde se busca chegar ao criminoso utilizando de meios legais, a geolocalização é uma tarefa extremamente complicada, ainda mais quando o criminoso ataca por meio da rede de terceiros, uma vez que os dados que podem ser obtidos não trazem grande precisão. Com um endereço de IP, por exemplo, o máximo que se consegue extrair é a cidade da qual o ato foi perpetrado, o que em uma cidade como São Paulo, é um dado quase irrelevante.

Em um cenário onde o atacante se comunica de alguma forma com a vítima e pode-se enviar informações ou analisar um perfil, por exemplo, é possível realizar o chamado *doxing*, na tentativa de inferir a localização e até a verdadeira identidade do malfeitor. Além disso, existem outros métodos que garantiriam o acesso a localização quase exata e a demais informações do atacante, como o *phishing*, o levando para um site malicioso no qual se poderia extrair informações, entretanto, tais métodos são ilegais, e, portanto, inviáveis.

Em adição a isso, dois métodos famosos em obras de ficção, mas que podem vir a ser bastante imprecisos na prática, são a triangulação por antenas de celular e a

16. A decisão se refere ao Marco Civil da Internet.

triangulação por servidores, ambas utilizam da mesma técnica, analisar o tempo de recebimento e resposta do dispositivo em relação a diferentes antenas de celular e ou servidores, na tentativa de estimar as suas respectivas distâncias do dispositivo, assim, chegando a uma localização relativamente próxima da real. No entanto, em função de barreiras físicas, áreas remotas, interferências, dispositivos de baixa qualidade, entre outros aspectos, essa estimativa pode conter uma imprecisão de quilômetros.

Em virtude dos fatos supracitados, a solução mais simples, em posse de dados como o endereço de IP utilizado no ataque, para a geolocalização do criminoso, é solicitar ao provedor as devidas informações a respeito do contratador do serviço.

3.6. PORTAS LÓGICAS DE ACESSO

Segundo o Instituto de Referência em Internet e Sociedade[17], a atual tecnologia amplamente utilizada pelos números de IP está na versão IPv4. Essa versão já esgotou seus números possíveis dos números de IP destinados à América Latina e Caribe por volta do ano de 2014. Tal situação de limitação dos números de IP já vinha sendo discutida desde os anos 90, e foram sugeridas novas versões para substituir o IPv4. A tecnologia escolhida foi o IPv6, que possui amplitude de números de IP bem superiores, podendo o IPv4 ser utilizado por cerca de 4.3 bilhões de dispositivos, enquanto que o IPv6 pode ser utilizado por 3.4×10^{33} endereços distintos.

Ocorre que a tecnologia do IPv6 ainda não foi totalmente implementada, e por isso, outra técnica tomou lugar para resolver o problema da escassez dos endereços de IP o *Network Address Translation* (NAT).

Na fase de desenvolvimento do IPv4, foi segregada uma certa quantidade de IPs para serem privados, que seriam usados em redes privadas fora da internet. Além dos IPs privados, um outro número de IPs públicos também foi criado, e esses IPs são utilizados para realizar a maior parte das conexões com a internet. A tecnologia do NAT supera o problema do esgotamento de IPs ao permitir que vários dispositivos em uma rede de IPs privados compartilhem apenas um único IP público quando estiverem conectados à internet.

17. Disponível em https://irisbh.com.br/wp-content/uploads/2017/11/Portas-Logicas-e-os-Registros-de-Acesso-IRIS-1.pdf . Acesso em 28 de junho de 2022.

Para que esse compartilhamento de IPs aconteça, o roteador, que pode ser doméstico ou aquele utilizado por um provedor de conexão de grande porte, realiza a função de intermediário entre a rede interna a ele conectada e a internet. Através da associação dos IPs privados utilizados na rede interna e um ou mais IPs públicos designados àquele roteador, o sistema NAT direciona os pacotes de dados que entram e saem por meio dele, utilizando-se de portas que o permitem identificar qual dispositivo se conecta com qual endereço externo. As portas são um número adicionado ao final do endereço IP, que permite ao NAT criar uma tabela de associações e viabilizar sua função.

Dessa forma, quando foi atribuído ao provedor de conexão certo número de IPs, mas esse provedor atende a um número muito maior de clientes e dispositivos do que tem de IPs, é necessário implementar um sistema NAT, para permitir que os dispositivos de seus clientes se comuniquem com a rede externa. Através do gerenciamento das portas lógicas, pode-se compartilhar um IP público entre vários dispositivos conectados, sabendo a origem e destino de cada pacote endereçado ao roteador. Mesmo que todos os pacotes sejam destinados a um mesmo endereço IP, são diferenciados pelo roteador do provedor, por meio da tabela de vinculação e das portas lógicas a eles anexadas.

Nesse contexto, o sistema NAT dificulta a identificação de um usuário específico, uma vez que o mesmo número de IP pode estar sendo utilizado por vários usuários simultaneamente. Então, diante de uma requisição judicial de identificação de um usuário de IP em determinado momento, o provedor de conexão terá vários possíveis usuários a fornecer ao juízo. Tal situação dificulta para a parte interessada identificar o investigado ou atacante.

Dessa forma, surge a dúvida de se o provedor de conexão também tem a obrigação de guardar e armazenar a porta lógica utilizada por um usuário, pois o MCI não obriga o provedor de conexão a guardar as portas lógicas.

Alguns tribunais, em especial o Tribunal de Justiça do Estado de São Paulo, tem entendido que o provedor de conexão também deve fornecer a porta lógica utilizada pelo usuário, a fim de identificar o terminal específico de onde se originou o ilícito[18].

18. TJSP; Agravo de Instrumento 2087084-15.2017.8.26.0000; Relator (a): J.L. Mônaco da Silva;

4. DISSIMULAÇÃO NO USO DO IP

Na grande maioria dos casos, o criminoso será experiente o suficiente para esconder alguns dos rastros do seu ataque, como mostrado nas seções anteriores, um dos meios que se utiliza para chegar ao atacante é o endereço IP utilizado para a conexão com dispositivo da vítima, sendo assim, discorreremos a seguir sobre como ele possa ter escondido esse dado e quais seriam as medidas possíveis para contornar esse obstáculo.

4.1. FERRAMENTAS COMUNS PARA ANONIMIZAÇÃO NA INTERNET

Primeiramente, cabe apresentar os meios mais utilizados para a ocultação de tráfego e endereço IP. A começar pelo mais famoso deles, a VPN (*Virtual Private Network*), quando utilizada, cria-se um túnel de conexão entre o cliente e o provedor VPN, nele, todo tráfego é encriptado e, antes de chegar ao endereço final, passa por um ou mais servidores VPN, que fazem o intermédio entre o cliente e o domínio que se queira acessar, dificultando o rastreio do IP, visto que todos os acessos serão feitos por meio do IP do servidor e não do usuário. Essa ferramenta tem se tornado cada vez mais comum, seja para acessar conteúdo restritos por região, contornar censura, ter mais privacidade, por segurança ao se conectar com redes públicas e até para fins de trabalho remoto. Em virtude disso, mesmo no caso, como o desse trabalho, de um criminoso pouco habilidoso, devido a essa popularidade, ainda é altamente provável que tal malfeitor utilize desse artifício.

Em adição, as demais ferramentas se comportam de maneira semelhante, os acessos são feitos através de intermediários entre o usuário inicial e o usuário final, podendo ou não conter criptografia. O TOR ("*The Onion Router*") da TOR Project,

Órgão Julgador: 5ª Câmara de Direito Privado; Foro Central Cível - 41ª Vara Cível; Data do Julgamento: 02/08/2017; Data de Registro: 03/08/2017. TJSP; Agravo de Instrumento 2168151-36.2016.8.26.0000; Relator (a): Beretta da Silveira; Órgão Julgador: 3ª Câmara de Direito Privado; Foro Central Cível - 22ª Vara Cível; Data do Julgamento: 25/11/2016; Data de Registro: 25/11/2016. TJSP; Apelação Cível 0004132-12.2015.8.26.0411; Relator (a): Eduardo Sá Pinto Sandeville; Órgão Julgador: 6ª Câmara de Direito Privado; Foro de Pacaembu - 1ª Vara; Data do Julgamento: 28/08/2017; Data de Registro: 28/08/2017.

Inc., por exemplo, comumente associado a *darkweb* e *deepweb*, funciona da seguinte forma: o cliente, em posse do software do TOR, se conecta a um *node*, e este, por sua vez, se conecta a outro que se conecta a outro, e assim sucessivamente até chegar ao usuário final, tudo isso sob camadas de encriptação, por isso o nome onion, em português, cebola, visto as várias camadas envolvidas.

Já o proxy, seja público ou residencial, não possui, necessariamente, encriptação, apenas intermediadores na conexão. O proxy residencial, em especial, pode estar se tornando um grande problema, pois os endereços de IP, utilizados para a conexão, não são de data centers ou clouds, isto é, eles não são amplamente conhecidos, serviços como a Netflix, que possui conteúdos diferentes em diferentes regiões do mundo, já reconhece a maioria dos IPs dos provedores de VPN mais comuns, assim, ela não corre risco de receber penalizações por questões de detenção de direitos autorais ou de transmissão em cada região. Já os serviços de proxy residencial, utilizam de dispositivos comuns, como dispositivos IoT, que possuem um endereço residencial para realizar o intermédio do tráfego na rede.

Vale ressaltar que os provedores de acesso a internet conseguem observar que o tráfego está encriptado o que expõe o uso desses métodos, mas não o conteúdo acessado, ademais, os sites e aplicações acessadas conseguem, na maioria das vezes, saber se o acesso está sendo feito através de um sistema TOR, uma VPN ou proxy, visto que os *nodes* finais são públicos.

4.2. IOT DO LADO DO ATACANTE

Os endereços IP residenciais são distribuídos e alocados, em sua maioria, por provedores de serviço de internet, para residências, isto é, para pessoas físicas e não empresas como os IPs fornecidos a servidores e data centers, tendo isso em vista, caso um usuário acesse uma aplicação na internet por esse tipo de endereço IP ela o reconhecerá como uma pessoa comum.

Nesse cenário, o número de provedores de serviço de proxy residencial - no qual o tráfego é realizado através de dispositivos conectados a uma rede com endereço IP residencial, como celulares, computadores ou equipamentos IoT - cresce cada vez mais, pois seus usuários são indistinguíveis de usuários comuns, o que outros serviços de ocultação de endereço IP pecam em oferecer, além disso, é uma excelente

ferramenta para ataques DDoS e mineração de dados na internet.

Um estudo conduzido por Xianghang Mi[19] apontou que 237.029 dos 547.497 endereços de IP coletados em cinco provedores de proxy residencial diferentes, pertenciam a sistemas IoT, como webcams, impressoras, gravadores de disco, entre muitos outros. Ademais, foram encontrados diversos hosts comprometidos, executando malwares e servindo como bots para atividades maliciosas.

Logo, observa-se que um atacante pode utilizar do serviço de terceiros para se ocultar na rede e ainda se conectar a dispositivos IoT comprometidos, podendo extrair diversos tipos de dados de uma vítima, como gravações de vídeo, dados pessoais, dados bancários, entre outros.

4.3. IDENTIFICANDO O VERDADEIRO IP

Quando um desses artifícios é utilizado para a ocultação na rede, dificilmente o IP verdadeiro será localizado, o intuito principal dessas ferramentas é a privacidade e a anonimidade.

Logo, de forma direta, isto é, por meio de informações coletadas no dispositivo da vítima, é, na maioria das vezes, impossível se chegar ao atacante original, na circunstância de um serviço de VPN ter sido utilizado, pode ser feita uma tentativa de comunicação com o provedor dessa VPN, todavia, assim como em outras situações apresentadas neste artigo, as diferentes jurisdições entre o Brasil e os países em que este provedor esteja localizado trazem grandes obstáculos à investigação.

Nos cenários em que a identificação do IP pode ser feita, utiliza-se de métodos que fogem do alcance de uma investigação privada, como doxing, acesso aos dados do provedor de VPN e do provedor de internet, acesso ao tráfego dos usuários, por meio das ISP e provedores de VPN, e até phishing, entre outros.

19. XIANGHANG, Mi X. FENG, Liao, B. Liu, X. WANG, F. Qian, Z. LI, S. ALRWAIS, L. SUN e Y. LIU. *Resident Evil: Understanding Residential IP Proxy as a Dark Service, 2019*. IEEE Symposium on Security and Privacy. Disponível em: <https://www.computer.org/csdl/proceedings-article/sp/2019/666000b185/1dlwhxAKYSc>. Acesso em 28 de junho de 2022.

4.4. VIABILIDADE DA CONTINUIDADE DA INVESTIGAÇÃO NESSES CASOS

Quando deparado com a situação descrita, é altamente improvável que a investigação continue por este caminho, em virtude das dificuldades expostas, caso somente dados da conexão possam ser extraídos a única decisão cabível é recorrer à justiça. Caso contrário, se houve algum tipo de comunicação como e-mail, ligação ou mensagem, se há suspeitas de conhecidos da vítima, ou outra pista, possivelmente a investigação seguirá o curso normal de uma perícia forense não computacional. Não cabe no escopo deste trabalho detalhar a continuidade da investigação neste caso.

5. REPARAÇÃO DAS PERDAS E DANOS DA VÍTIMA

O objetivo primordial de uma investigação é chegar em um suspeito identificado e fazer com que este sujeito pague pelas condutas lesivas que realizou, tudo dentro das regras de um Estado Democrático de Direito, com direito ao devido processo legal e contraditório. Assim, civilmente, é natural o interesse da vítima em mitigar as próprias perdas e requerer no Poder Judiciário os seus direitos.

Uma vez constatado o dano e identificado o responsável pelo ataque, a parte prejudicada pode requerer judicialmente a reparação por todos os prejuízos decorrentes daquela situação.

O Código Civil (CC) determina o que é ato ilícito no art. 186[20]. Ainda de acordo com essa lei, quem comete o ato ilícito está sujeito à reparação dos danos por ele causados, conforme dispõe o art. 927[21]. Nesse sentido, essa reparação deve ser integral, de acordo ao dano sofrido, nos termos do art. 944[22] do CC.

Então, remontando toda a investigação do ataque e os elementos de prova adquiridos nesse procedimento, a vítima deve demonstrar ao juízo competente toda a maneira como o ataque ocorreu, fazendo a ligação entre o atacante e o dano sofrido.

20. Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
21. Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
22. Art. 944. A indenização mede-se pela extensão do dano.

Essa ligação entre o atacante e o dano é chamada de nexo de causalidade. O nexo de causalidade pode ser conceituado como a "ligação jurídica realizada entre a conduta ou atividade antecedente e o dano, para fins de imputação da obrigação ressarcitória[23]".

Dessa forma, a vítima pode demonstrar seu prejuízo em algum dano a equipamento, vazamento de dados ou violação de seus direitos da personalidade, fazendo o nexo causal através do IP utilizado pelo terminal do atacante. Todos esses elementos serão analisados pelo juiz de direito e ele poderá determinar a eventual responsabilização do atacante naquele caso, o que pode gerar o direito da vítima em ter reparado o dano que sofreu.

Caso o atacante seja de fora do Brasil, a solução jurídica torna-se muito mais complexa, pois envolveria cooperação internacional de outro país, e cada Estado tem leis próprias para resolver esse tipo de lide. Portanto, não abordaremos aqui neste trabalho a situação de o atacante estar localizado fora do território brasileiro.

6. CONCLUSÃO

A partir da pesquisa elaborada observa-se que é possível fazer uma investigação de caráter civil sobre quem foram os responsáveis por um ataque cibernético, entretanto, caso o atacante seja alguém versado em tecnologia da informação e conheça meios para dissimular e esconder sua ação, a investigação provavelmente será infrutífera.

As várias formas de se esconder na internet podem tornar uma investigação muito custosa, envolvendo países, empresas e tecnologias distintas, tornando o trabalho do investigador muito complexo, custoso e demorado.

Diante disso, observa-se que o ideal é cooperação entre os diferentes países, através de meios uniformes para viabilizar o rastreamento de criminosos, tal como a Convenção de Budapeste.

23. MULHOLLAND, Caitlin Sampaio. *A responsabilidade civil por presunção de causalidade*. Rio de Janeiro, GZ Editora, 2010, p. 57.

REFERÊNCIAS

AMAZON, *Definição de APIs* Disponível em https://aws.amazon.com/pt/what-is/api/#:~:text=API%20significa%20Application%20Programming%20Interface,de%20servi%C3%A7o%20entre%20duas%20aplica%C3%A7%C3%B5es. Acesso em 28 de junho de 2022.

BRASIL. **Constituição** (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018.

CRETELLA JÚNIOR, José. Comentários à Constituição brasileira de 1988. 3. ed. Rio de Janeiro : Forense Universitária, v. 1, 1992.

DIDIER JR, Fredie. Curso de direito processual civil. Juspodivm: Salvador, 11ª Ed., p. 83. 2008.

GOVERNO DO ESTADO DO MATO GROSSO DO SUL. Crimes virtuais: MS registrou mais de 3,5 mil ocorrências em 2021. Disponível em: <http://www.ms.gov.br/crimes-virtuais-policia-de-ms-registrou-mais-de-35-mil-ocorrencias-em-2021-neste-ano-ja-sao-1-126-casos/#:~:text=Em%20Mato%20Grosso%20do%20Sul,j%C3%A1%20foram%20registrados%201.126%20casos>. Acesso em 22 de junho de 2022.

ÍRIS-BH. *Portas lógicas e registros de acesso*. Disponível em https://irisbh.com.br/wp-content/uploads/2017/11/Portas-Logicas-e-os-Registros-de-Acesso-IRIS-1.pdf . Acesso em 28 de junho de 2022.

JANARTHANAN, Tharmini. *IoT Forensics: An Overview of the Current Issues and Challenges*. Disponível em: < https://www.researchgate.net/publication/347479384_IoT_Forensics_An_Overview_of_the_Current_Issues_and_Challenges>. Acesso em 28 de junho de 2022.

KASPERSKY. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address>. Acesso em 23 de junho de 2022.

MONTASARI, Reza; JAHANKHANI, Hamid; Digital Forensic *Investigation of Internet of Things (IoT) Devices: Advanced Sciences and Technologies for Security Applications*. Londres: Springler, 1ª edição, 2021.

MULHOLLAND, Caitlin Sampaio. A responsabilidade civil por presunção de causalidade. Rio de Janeiro, GZ Editora, 2010, p. 57.

M. Yu, J. Zhuge, M. Cao, Z. Shi and L. Jiang, "*A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices*", *Future Internet*, vol. 12, no. 2, p. 27, 2020.

MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS. Disponível em : <https://www.mpmg.mp.br/portal/menu/comunicacao/noticias/estelionato-digital-mpmg-intensifica-atuacao-para-combater-golpes-pelowhatsappem-mg-8A9480687CE-BDB46017CF0ECEB305789-00.shtml#:~:text=Em%20Minas%20Gerais%2C%20conforme%20levantamento,aplicado%20pelo%20aplicativo%20no%20estado>. Acesso em 22 de junho de 2022.

ORIWOH, Ewede. Disponível em https://www.researchgate.net/publication/258093766_Internet_of_Things_Forensics_Challenges_and_Approaches . Acesso em 28 de junho de 2022.

TJSP; Agravo de Instrumento 2168151-36.2016.8.26.0000; Relator (a): Beretta da Silveira; Órgão Julgador: 3ª Câmara de Direito Privado; Foro Central Cível - 22ª Vara Cível; Data do Julgamento: 25/11/2016; Data de Registro: 25/11/2016.

TJSP; Agravo de Instrumento 2087084-15.2017.8.26.0000; Relator (a): J.L. Mônaco da Silva; Órgão Julgador: 5ª Câmara de Direito Privado; Foro Central Cível - 41ª Vara Cível; Data do Julgamento: 02/08/2017; Data de Registro: 03/08/2017.

TJSP; Apelação Cível 0004132-12.2015.8.26.0411; Relator (a): Eduardo Sá Pinto Sandeville; Órgão Julgador: 6ª Câmara de Direito Privado; Foro de Pacaembu - 1ª Vara; Data do Julgamento: 28/08/2017; Data de Registro: 28/08/2017.

TUDO O QUE VOCÊ SEMPRE QUIS PERGUNTAR SOBRE O CHECKM8 E O CHECKRA1N. Disponível em: <https://periciacomputacional.com/tudo-o-que-voce-sempre-quis-perguntar-sobre-o-checkm8-e-o-checkra1n/>. Acesso em 28 de junho de 2022.

XIANGHANG, Mi X. FENG, Liao, B. Liu, X. WANG, F. Qian, Z. LI, S. ALRWAIS, L. SUN e Y. LIU. *Resident Evil: Understanding Residential IP Proxy as a Dark Service*, 2019. IEEE Symposium on Security and Privacy. Disponível em: <https://www.computer.org/csdl/proceedings-article/sp/2019/666000b185/1dlwhxAKYSc>. Acesso em 28 de junho de 2022.

III
INTERNET DAS COISAS E PROTEÇÃO DE DADOS PESSOAIS

O VAZAMENTO DE DADOS PESSOAIS NA INTERNET DAS COISAS (IOT) E A APLICABILIDADE PRÁTICA DO *PRIVACY BY DESIGN* E DO *PRIVACY BY DEFAULT*

Renata Capriolli Zocatelli Queiroz

Advogada. Pós-Doutoranda e Doutora pela Faculdade de Direito da Universidade de São Paulo – USP. Mestre e especialista pela Universidade Estadual de Londrina - UEL. Professora Convidada do Programa de Mestrado Profissional em Direito, Sociedade e Tecnologia da Escola de Direito das Faculdades Londrina. Professora da Pós-Graduação em Direito Empresarial aplicado à era Digital da Universidade Estadual de Londrina. Professora da Faculdades Londrina.

Adriana Cardoso de Moraes Cansian

Advogada Especialista e Direito Digital. Doutora em Direito Comercial.

Caio Henrique de Moraes Cintra

Advogado Especialista em Direito Digital e Proteção de Dados pela Escola Brasileira de Direito – EBRADI. Certificado EXIN Privacy and Data Protection Essentials based on LGPD. Coautor do Livro LGPD x Campanha Eleitoral: Perspectivas e Desafios.

DOI: https://doi.org/10.59224/dti5.ch7

Resumo: Embora o mercado de dispositivos ligados à Internet das Coisas siga em amplo crescimento, nota-se que o nível de segurança da informação empregado na construção dos equipamentos permanece abaixo do aceitável, com altas possibilidades de exploração de suas vulnerabilidades e comprometimento dos dados. Assim, o presente artigo tem por objetivo propor a utilização de técnicas amplamente empregadas na proteção de dados como o *Privacy by Design*, garantindo

Abstract: *Although the market for devices connected to the Internet of Things continues to grow, it is noted that the level of information security employed in the construction of equipment remains below acceptable, with high possibilities of exploitation of its vulnerabilities and compromise of data. Thus, this article aims to propose the use of techniques widely used in data protection such as Privacy by Design, ensuring a higher level of*

maior nível de segurança desde a concepção dos dispositivos, sem o comprometimento de suas funcionalidades. Utiliza o método dedutivo na análise dos principais casos de vazamentos de dados envolvendo dispositivos IoT e aplicação da abordagem descritiva e conclui que a aplicação de técnicas destinadas a garantir a privacidade e proteção de dados tem o poder de mitigar os riscos de incidentes de segurança envolvendo o uso de IoT.

Palavras-chave: IoT; Vazamento de Dados; Privacy by Design.

security from the design of the devices, without compromising their functionality. It uses the deductive method in the analysis of the main cases of data leaks involving IoT devices and the application of the descriptive approach and concludes that the application of techniques aimed at guaranteeing privacy and data protection has the power to mitigate the risks of security incidents involving the use of IoT.

Keywords: *IoT; Data Breach; Privacy by Design.*

INTRODUÇÃO

Dispositivos IoT seguem em constante crescimento global. De acordo com relatório da empresa alemã IoT Analytics, projeta-se que, até o ano de 2025, mais de 27 bilhões de dispositivos estejam conectados à internet das coisas[1]. Naturalmente, em razão do volume, a tecnologia também movimenta vultuosas quantias. Dados coletados pela consultoria americana McKinsey demostram um potencial econômico de até US$ 12,6 trilhões[2].

1. IOT ANALYTICS. Insights Release State of IoT Spring 2022. Disponível em: https://h9e3r9w2.rocketcdn.me/wp/wp-content/uploads/2022/05/Insights-Release-State-of-IoT-Spring-2022.pdf. Acesso em: 01 fev. 2023.
2. MCKINSEY & COMPANY The Internet of Things Catching up to na accelerating opportunity. Disponível em: <https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf>. Acesso em: 01 fev. 2023.

No entanto, não obstante todo o valor movimentado, dispositivos IoT costumam apresentar graves problemas de segurança. Em grande parte, por falta de investimento ou por receio dos fabricantes em prejudicar a usabilidade.

A falta de Segurança da Informação, combinada com a grande quantidade de dados tratados por dispositivos IoT, pode causar sérias ameaças à privacidade e proteção dos dados pessoais de seus usuários, inclusive nas situações em que dados delicados, como de saúde, genéticos ou biológicos são tratados.

Conforme se apresentará ao longo deste artigo, incidentes de segurança já foram registrados e as consequências da ausência de requisitos básicos de proteção da tecnologia vêm sendo debatidas por inúmeros países, inclusive com a propositura de projetos de lei que visam a estabelecer obrigações aos fabricantes e desenvolvedores.

Por esta razão, o presente trabalho tem como proposta o debate sobre as vulnerabilidades de segurança presentes nos sistemas e dispositivos conectados à internet das coisas, bem como na possibilidade da utilização dos princípios de Privacy By Design e Privacy By Default como meio de mitigar a possibilidade de incidentes de segurança envolvendo dados pessoais.

1. O DIREITO À PROTEÇÃO DE DADOS PESSOAIS

A popularização do acesso à internet proporcionou diversas mudanças sociais. Impactou a forma com a qual o ser humano se relaciona, trabalha, se diverte, consume e vive. Trouxe diversos benefícios, porém, também implicou em riscos à humanidade.

A partir do acesso à grande rede, o indivíduo passou a expor fragmentos da sua vida e, com isso, *big datas* passaram a ser formados armazenando todas essas informações. Diante disso, necessário se demonstra a efetiva proteção aos dados pessoais[3].

3. "Se, por um lado a preocupação com o tema não é nova; por outro, o desenvolvimento tecnológico das últimas décadas, principalmente com a invenção dos computadores pessoais e da internet, trouxe uma miríade de problemas e questionamentos referentes à privacidade, anteriormente inimagináveis. A internet relativizou distâncias, permitindo a comunicação praticamente instantânea entre partes opostas do mundo, com som e imagens de alta definição. E juntamente, com os benefícios, o progresso tecnológico trouxe também novos riscos". (PARENTONI, Leonardo. O Direito ao Esquecimento [Right to Oblivion]. *In*: DE LUCCA, Newton; SIMÃO FILHO,

Cumpre mencionar que a coleta de dados não é algo novo, porém, o avanço da tecnologia e o uso da inteligência artificial potencializaram o tratamento dos dados devido à capacidade de processamento de dados da máquina, uma vez que não se cansa ao realizar o processamento dos dados[4]. Como exemplo, pesquisas[5] afirmam que, com 250 curtidas, os algoritmos são capazes de saber mais sobre uma pessoa do que seu companheiro.

Em 2017, a Revista *The Economist*[6] já apontava os dados como o novo petróleo do Século XXI. Na capa publicada em 6 de maio de 2017, a manchete anunciava – "*The world's most valuable resource*" – "O recurso mais valioso do mundo", demonstrando que os dados se tornaram insumos essenciais para o desenvolvimento das atividades econômicas, o que criou uma economia movida a dados.

Diante desse cenário, resta claro que a proteção dos dados pessoais não diz respeito tão somente à tutela da autodeterminação, mas também à tutela do Estado Democrático de Direito. Com isso, emerge a necessidade da criação de legislações que tutelem sobre a proteção dos dados pessoais[7].

No que tange à proteção de dados pessoais, cumpre ressaltar o protagonismo Europeu na produção de legislações sobre o tema desde os anos de 1970, quando o

---

Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). *Direito & Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015, p. 540).

4. TOMASEVICIUS FILHO, Eduardo. Inteligência artificial e direitos da personalidade: uma contradição em termos? *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, v. 113, pp. 133-149, 2018. Disponível em: https://www.journals.usp.br/rfdusp/article/view/156553. Acesso em: 3 dez. 2022.
5. LISSARDY, Gerardo. "Despreparada para a era digital, a democracia está sendo destruída", afirma o guru do "big data". *BBC News Brasil*, 9 abr. 2017. Disponível em: https://www.bbc.com/portuguese/geral-39535650. Acesso em: 28 nov. 2022.
6. THE WORLD'S most valuable resource is no longer oil, but data. *The Economist*, 6 maio 2017. Disponível em: www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 28 nov. 2022.
7. "Os avanços tecnológicos dos últimos anos, com as novas tecnologias da informação, vieram para alterar de forma permanente o mundo que nos rodeia e trouxeram a necessidade de uma legislação de proteção dos dados pessoais que buscasse o equilíbrio entre a garantia das liberdades e direitos individuais e que se traduz na reserva da intimidade da vida privada e a liberdade de circulação da informação pessoal". CARLOTO, Selma. *A lei geral de proteção de dados*: enfoque nas relações de trabalho. 2. ed. São Paulo: LTr, 2021, p. 115.

estado de Hesse, na Alemanha, aprovou a primeira lei de proteção de dados do mundo[8].

Desde então a União Europeia vem publicando normativas com o objetivo de tutelar a proteção dos dados pessoais, sendo fato que seu pioneirismo causou impacto nas demais legislações ao redor do mundo, em especial após entrar em vigor o *General Data Protection Regulation* (GDPR) – Regulamento Europeu de Proteção de Dados, uma vez que seu art. 45 exige nível protetivo adequado para transação internacional de dados.

Sobre o assunto, Cristina Caldeira[9] afirma: *"podemos observar que a matéria de proteção de dados pessoais ocupa um lugar central na legislação da União Europeia, e que o impacto do novo instrumento criado vai além da Europa".*

No Brasil não foi diferente. Após a entrada em vigor do GDPR, no dia 25 de maio de 2018, em agosto do mesmo ano a Lei Geral de Proteção de Dados foi publicada e, antes de comentar sobre os princípios contidos na LGPD, oportuno se torna destacar a EC 115/2022, a qual elevou à categoria de direito fundamental a proteção dos dados pessoais no Brasil e conferiu competência privativa à União para legislar sobre a matéria, publicada em fevereiro de 2022.

A LGPD, em seu art.1º, deixa claro que essa lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Seu objetivo é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Trata-se de uma lei fundada em questões práticas, de ordem jurídica, técnica e administrativa, uma vez que a proteção dos dados pessoais é uma jornada multidisciplinar. Os princípios nela contidos são práticos, de modo que, a partir da sua observância, a efetiva tutela da proteção dos dados pessoais se concretize.

---

8. DOHMANN, Idra Spiecker Gen. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *In:* DONEDA, Danilo *et al. Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 113.
9. CALDEIRA, Cristina. A proteção de Dados Pessoais e o Impacto nas Transferências Internacionais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). *Direito & Internet IV*: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019, p. 634.

O caput do art. 6[10] e seus incisos expressam os princípios dispostos na lei, dentre os quais, para fins de objeto de estudo desta pesquisa, destaca-se o princípio da prevenção, art. 6º, III, o qual impõe a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento dos dados pessoais.

Ressalta-se que no decorrer da lei é possível encontrar outros princípios dispostos em outros dispositivos, assim como *privacy by default* e o *privacy by design,* expressamente dispostos, respectivamente, no art. 46, caput, e art. 46, § 2º.

O art. 46, caput, exige dos agentes de tratamento a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Já o art. 46, § 2º da LGPD, impõe a observância das regras do contido na lei desde a concepção do

10. "Art. 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". (BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 2 dez. 2022).

produto até sua execução.

Ou seja, a LGPD prevê a formulação de regras de boas práticas e de governança, possibilitando aos agentes de tratamento o estabelecimento de condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Desta forma, o próximo capítulo abordará a segurança da informação aplicada à proteção dos dados pessoais a partir da prática do *privacy by design* e do *privacy by default* a partir do uso da internet das coisas, de modo a esclarecer a relevância de sua aplicabilidade face à ocorrência de violação a partir da apresentação do estudo de caso concreto, conforme será abordado no terceiro capítulo.

2. O CONCEITO DE IOT E OS DADOS TRATADOS

Antes de adentrar especificamente aos conceitos de segurança da informação aplicáveis aos dispositivos ligados à internet das coisas, é fundamental que se estabeleça o conceito de IoT, apresentando ainda um panorama dos dados comumente tratados em suas operações.

De acordo com o *European Research Cluster on the Internet of Things – IERC,* a internet das coisas pode ser definida como "*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network".*[11]

Em definição formulada pelo Grupo de Estudos em Direito e Tecnologia da Universidade Federal de Minas Gerais – DTEC – UFMG, a "*IoT Opera em rede com*

11. EUROPEAN Research Cluster on the Internet of Things – IERC. *Internet of Things*. Disponível em: < http://www.internet-of-things-research.eu/about_iot.htm#:~:text=The%20IERC%20definition%20states%20that,use%20intelligent%20interfaces%2C%20and%20are> Acesso em: 29 jan. 2023.

utilização de qualquer protocolo, de sensores e por meio de uma programação prévia com substituição da ação humana. As 'coisas' irão operar numa rede, e, por meio de uma programação prévia, oferta/demanda de bens e serviços será realizada".[12]

Por meio dos conceitos acima apresentados, é possível concluir que a Internet das Coisas é responsável pela transmissão de dados coletados através de sensores existentes em dispositivos voltados para as mais diversas atividades domésticas, médicas ou industriais.

Há uma infinidade de dispositivos médicos que utilizam a internet das coisas como tecnologia base de sua atuação, a exemplo de sensores que monitoram os sinais vitais de um paciente internado e bombas de infusão que, através de resultados analíticos, ministram a quantidade adequada de medicação e até mesmo realizam o monitoramento remoto de pacientes crônicos ou de longo prazo. Esses dispositivos são conhecidos como *Internet of Medical Things - IoMT*[13].

Outros dispositivos, como os *weareables,* dispositivos tecnológicos que dispõem da forma de peças vestíveis, como o caso de *smartwatches*, pulseiras ou óculos de realidade virtual, embora não sejam equipamentos médicos propriamente ditos, detectam, armazenam e transmitem dados de saúde de seus usuários, como batimentos cardíacos, qualidade de sono e exercícios realizados.

Já veículos autônomos tratam e armazenam dados que compreendem a localização de carro e, consequentemente, de seu usuário, em tempo real, bem como as rotas utilizadas para chegar em casa ou ao trabalho.

Uma das principais características da internet das coisas consiste no alto volume de dados tratados que, em sua maioria, servem de indicadores para que os dispositivos avaliem e monitorem os dados de sua atuação, enviando alertas para que ações

12. GRUPO DE ESTUDOS em Direito e Tecnologia da Universidade Federal de Minas Gerais – DTEC – UFMG. IoT e Proteção de Dados Pessoais. 23/11/2021. Disponível em: < https://www.dtibr.com/post/iot-e-prote%C3%A7%C3%A3o-de-dados-pessoais> Acesso em: 29 jan. 2023.
13. IoMT (Internet of Medical Things) or healthcare IoT. TechTarget. Disponível em: https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things#:~:text=Examples%20of%20IoMT%20include%20remote,can%20send%20information%20to%20caregivers.> Acesso em 29 jan. 2023.

específicas sejam adotadas em casos de anomalias detectadas, por exemplo.

Há uma série de outros exemplos possíveis de dispositivos IoT que tratam dados pessoais como localização, dados pessoais para confirmação de pagamentos, gênero, endereços eletrônicos, dentre outros.

2.1. DA AUSÊNCIA DE IMPLEMENTAÇÃO DA SEGURANÇA DA INFORMAÇÃO NOS DISPOSITIVOS IOT

Conforme anteriormente mencionado, há um grande tráfego de informações e dados pessoais nos dispositivos conectados à internet das coisas, incluindo dados sensíveis relacionados à saúde de seus usuários, sendo necessária a adoção de elementos voltados à Segurança da Informação desde a fase de projeto dos dispositivos.

A segurança da informação pode ser definida como a implementação de meios capazes de garantir a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar seus riscos e maximizar o retorno sobre os investimentos e as oportunidades de negócio[14].

Há três princípios que podem ser considerados como fundamentais para a segurança da informação: a Confidencialidade, a Integridade e a Disponibilidade das informações em questão. A confidencialidade é responsável por garantir que apenas as pessoas autorizadas tenham acesso às informações protegidas, garantindo, assim, que não haja o acesso de tais informações por pessoa não autorizada, o que caracterizaria um vazamento de dados/informações.

A integridade visa a garantir que não haja qualquer modificação indevida na informação/dado, devendo este permanecer o mesmo durante todo o seu tratamento, sendo alterado apenas por quem possui tal direito.

A disponibilidade, por sua vez, é a garantia de que a informação estará disponível sempre que for consultada, isto é, que não permanecerá inacessível às partes autorizadas no momento de sua utilização/tratamento.

Na segurança para os dispositivos conectados à internet das coisas, o tratamento deve ser o mesmo, abordando sempre o aspecto tecnológico, de processo e de

14. HINTZBERGEN, Jule [et al.]. *Fundamentos de segurança da informação:* com base na ISO 27001 e na ISO 27002; tradução Alan de Sá – Ed. Brasport, Rio de Janeiro, 2018.

pessoas, com a manutenção dos princípios básicos da Segurança da Informação, adaptando-se ao uso dessa tecnologia[15].

Infelizmente, em grande parte das vezes, dispositivos IoT não contam com um nível de segurança da informação condizente com a importância dos dados tratados. Um relatório publicado pela Claroty, empresa ligada à segurança de dispositivos médicos (IoMT's), concluiu que a publicação de vulnerabilidades que atinge dispositivos móveis aumentou em 57% primeiro semestre de 2022[16]. Outro relatório, produzido pela Cynerio, revela ainda que a indústria hospitalar é a indústria mais visada para ataques do tipo *ransomware*, absorvendo de 100 a 200% mais ataques que a segunda categoria de negócios[17].

Segundo o Microsoft Digital Defense Report 2022[18], a utilização de senhas fracas em dispositivos IoT compromete a segurança de toda a rede, inclusive em sua utilização industrial.

Outro fator que enfraquece a segurança dos dispositivos conectados à internet das coisas é uma preocupação com eventual comprometimento de sua usabilidade, posto que grande parte dos dispositivos são de uso contínuo do titular de dados, como pulseiras e relógios inteligentes[19].

---

15. MORAES, Alexandre de. *Segurança em IoT*: entendendo os riscos e as ameaças em IoT. Alexandre de Moraes, Victor Takashi Hayashi – Rio de Janeiro, RJ: Alta Books, 2021.
16. STATE of XIoT Security. T82 – The Claroty Research Team. Disponível em: <https://web-assets.claroty.com/resource-downloads/team82-state-of-xiot-1h-2022-1661181434.pdf> Acesso em: em 29 jan. 2023.
17. CYNERIO Research Report. The State of Healthcare IoT Device Security 2022. Acesso em: 29 jan. 2023.
18. MICROSOFT Digital Defense Report 2022. Disponível em: < https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us>. Acesso em: 30 jan. 2023.
19. Nesse sentido: "[...] Além disso, uma conhecida premissa de desenvolvimento também permeia os processos de desenvolvimento de dispositivos conectados por IoT, qual seja: segurança é inversamente proporcional à usabilidade. De fato, prioriza-se muito mais um sistema que seja fácil de ser usado ou até mesmo intuitivo, àqueles que necessitam de manuais de instrução, por exemplo. O produto para ser escalável precisa ser intuitivo, fácil de ser usado e prático e escalabilidade é uma característica fundamental no mercado de tecnologia". CANSIAN, Adriana Cardoso de Moraes. *Aspectos Jurídicos Relevantes da Internet das Coisas (IoT):* Segurança e Proteção de Dados; Adriana Cardoso de Moraes Cansian; orientador Newton De Lucca; Demi Getschko - São Paulo,

Não faltam casos que corroborem com os problemas de segurança apontados pelos relatórios. Em janeiro de 2023, pesquisadores de uma empresa de segurança encontraram vulnerabilidades em placas veiculares digitais que estavam em teste na California. O produto promete mais praticidade e segurança, já que poderia identificar veículos roubados, além de não ser mais necessário que os motoristas colem adesivos em suas placas para identificar que a situação do veículo está regular. Entretanto, as vulnerabilidades encontradas permitiram que os pesquisadores pudessem monitorar a localização de todos os veículos que estavam utilizando a placa, tivessem acesso e possibilidade de alteração a todos os dados dos proprietários dos carros, e ainda pudessem alterar a numeração das placas[20].

Outras vulnerabilidades já foram encontradas anteriormente em veículos autônomos, em que, embora o ataque não desse controle do carro ao invasor, possibilitava que portas fossem destravadas e outras funções habilitadas[21].

Nos dispositivos médicos, por sua vez, os registros de ataques de *ransomware* que afetam equipamentos clínicos conectados à rede tiveram início em maio de 2017, quando o malware conhecido como *WannaCry* afetou uma série de equipamentos radiológicos em diversos hospitais americanos, comprometendo o tratamento de pacientes com câncer que estavam em tratamento de radiologia[22].

Diante de vários outros casos em que a Segurança da Informação foi comprometida por falhas do gênero, em setembro de 2022, foi apresentada pelo Comissão Europeia uma proposta de regulamento sobre requisitos de segurança a serem contemplados pelos fabricantes de softwares e hardwares comercializados nos países da União Europeia, incluindo dispositivos IoT. O Cyber Resilience Act, como a

---

2022.

20. JALOPNIK. *Researchers Hacked California's Digital License Plates, Gaining Access to GPS Location and User Info (Update).* Disponível em: <https://jalopnik.com/researchers-hacked-californias-digital-license-plates-1849966295?utm_source=twitter&utm_medium=SocialMarketing&utm_campaign=dlvrit&utm_content=jalopnik> Acesso em 30 jan. 2023.
21. CNN. *Teen's Tesla hack shows how vulnerable third-party apps may make cars.* Disponível em: < https://edition.cnn.com/2022/02/02/cars/tesla-teen-hack/index.html> Acesso em: 30 jan. 2023.
22. FORBES. *Medical Devices Hit By Ransomware For The First Time In US Hospitals.* Disponível em: <https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/?sh=2486e603425c>. Acesso em: 01 fev. 2023.

proposta ficou conhecida, é a primeira proposta de legislação europeia a estabelecer requisitos mínimos de segurança, estabelecendo como responsabilidade de seus fabricantes o monitoramento das vulnerabilidades dos dispositivos, bem como as atualizações de segurança necessárias para saná-las[23].

3. A IMPORTÂNCIA DO *PRIVACY BY DESIGN* E DO *PRIVACY BY DEFAULT* NO DESENVOLVIMENTO DE DISPOSITIVOS IOT

Para corrigir as questões da ausência da implementação de segurança mencionadas no tópico anterior, é fundamental que fabricantes e desenvolvedores passem a adotar práticas padronizadas já no início da concepção de um novo produto. Nesse sentido, há um conceito que, se corretamente observado, mitiga o risco de incidentes de segurança e do vazamento de dados pessoais. Trata-se do Privacy by Design.

Referido conceito foi desenvolvido por Ann Cavoukian, referência em privacidade e proteção de dados e ocupante do cargo de Comissária de Informação e Privacidade da cidade de Ontário, no Canadá, entre os anos de 1997 e 2014. Na década de 1990, Ann notou que, com o avanço das tecnologias que tornavam o mundo cada vez mais interconectado, as leis não teriam, por si só, o condão de garantir efetiva proteção à privacidade dos titulares, sendo fundamental que as empresas incorporassem ainda no desenvolvimento de seus projetos medidas voltadas à garantia do direito à privacidade[24].

Posteriormente, o conceito trazido por Ann se tornou padrão entre autoridades e pesquisadores de Privacidade e Proteção de Dados, sendo posteriormente mencionado pela Consideranda 46 da Diretiva 95/46 da União Europeia, pela Consideranda 78 e pelo artigo 25 do General Data Protection Regulation – GDPR e incorporado pela Lei nº 13.709/2012 (Lei Geral de Proteção de Dados) no Brasil.

Já em 2009, a Autora escreveu um artigo com o título: *Privacy by Design. The 7*

23. LEAK: *Commission to introduce cyber requirements for Internet of Things products*. Euroactiv. Disponível em: <https://www.euractiv.com/section/cybersecurity/news/leak-commission-to-introduce-cyber-requirements-for-internet-of-things-products/>. Acesso em 30 jan. 2023.

24. LGPD: Lei Geral de Proteção de Dados Pessoais comentada, p. 362, / coordenadores Viviane Nóbrega Maldonado e Renato Ópice Blum – 3ª ed. rev., atual. e ampl. – São Paulo, Thomson Reuters Brasil, 2021.

Foundational Principles[25], que traz os sete princípios básicos do Privacy By Design a serem seguidos pelas empresas fabricantes. São eles:

> i. Proativo, não reativo; preventivo, não corretivo: este princípio aborda a necessidade de que os fabricantes já implementem medidas prévias a fim de garantir a proteção da privacidade dos usuários desde a elaboração do projeto, e não no momento da detecção de um incidente de segurança ou em remediação após o vazamento dos dados.
>
> ii. Privacidade definida por padrão: o objetivo desse princípio é que os produtos já venham habilitados de maneira a garantir a privacidade completa do usuário, não sendo necessária qualquer configuração adicional por parte deste.
>
> iii. Privacidade embutida no sistema: durante o desenvolvimento do produto, a privacidade deve ser tida como um dos elementos centrais, sendo um dos motivos de preocupação central do início ao término do desenvolvimento do produto/serviço.
>
> iv. Funcionalidade completa: A escolha do usuário por proteger sua privacidade não deve privá-lo de qualquer funcionalidade disponível, evitando, assim, que o usuário tenha que se perguntar se prefere determinada funcionalidade ou a garantia de sua privacidade.
>
> v. Segurança durante todo o ciclo de vida da informação: este princípio tem grande relação com o estudo apresentado no presente artigo, pois trata do dever que os sistemas de informação devem garantir do início ao término do tratamento de dados. No caso dos dispositivos IoT, esse princípio ganha ainda mais força, em razão da natureza dos dados tratados, conforme abordado no tópico anterior. Por esta razão, a implementação de requisitos de Segurança da Informação, elementos que visam a garantir a integridade, confidencialidade e disponibilidade dos dados tratados pelos dispositivos desde o momento de seu projeto, é fundamental e aumenta consideravelmente a segurança de seu uso.
>
> vi. Transparência com o titular: os fabricantes devem manter uma relação que privilegie a transparência, deixando claro aos titulares seus processos e políticas sobre como sua governança é conduzida.
>
> vii. Respeito pela privacidade como tema central: a privacidade do usuário deve ser tida como elemento de preocupação central dos fabricantes, atendendo aos seus

25. O conteúdo original, em inglês, pode ser acessado em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

anseios tanto em relação à performance quanto em relação à garantia de sua privacidade.

O princípio do *Privacy by Default*, que se refere à aplicação das medidas mais restritivas proporcionadas pelo produto/serviço como padrão, pode ser apontado como um princípio derivado do próprio *Privacy by Design*, tendo em vista se tratar de uma prática englobada.

Dessa forma, verifica-se que a adoção dos conceitos de *Privacy by Default* e *Privacy by Design* no projeto e construção dos dispositivos e sistemas contemplam a segurança dos titulares de dados, garantindo que, desde a concepção do produto/serviço, haja uma preocupação relacionada à garantia da privacidade, por meio da adoção de técnicas e projetos adequados.

CONCLUSÃO

Diante de todo o contexto apresentado, é possível verificar que a internet das coisas é uma tecnologia relativamente nova e em ampla expansão no Brasil e no mundo, ganhando mais dispositivos e usuários com o passar dos anos. Nota-se, ainda, que referida tecnologia tem por característica a coleta e interpretação de dados, muitas vezes de natureza pessoal, a fim de estabelecer parâmetros de controle e cumprir com sua função.

Da mesma maneira, é possível verificar que a grande maioria dos dispositivos não apresenta um nível aceitável de segurança, proporcionando terreno fértil para que agentes maliciosos possam realizar ataques e vazar dados de diversas naturezas.

Com o objetivo de mudar o cenário e implementar maior segurança, diversos países têm se movimentado na edição de leis que estabelecem níveis mínimos de proteção de dados e informações nos sistemas e aplicativos, a exemplo da edição do *Cyber Resilience Act* por parte da União Europeia, que faz com que os fabricantes se tornem responsáveis pela manutenção da segurança e criação de correções de falhas.

Para que um sistema ou aplicativo apresente um alto nível de segurança, a melhor forma de conduzir o assunto é incluir a privacidade e a proteção de dados desde a fase de projeto, fazendo com que todas as suas funcionalidades tenham a segurança como um dos fatores fundamentais.

Nesse sentido, a aplicação do *Privacy by Design*, conceito criado por Ann Cavoukian na década de 1990, se amolda perfeitamente às necessidades, trazendo a visão protecionista ao cerne das criações, reforçada pelo conceito de que a proteção à privacidade deve ser utilizada por padrão (*Privacy by Default*), garantindo assim que, independentemente da familiaridade do titular com a tecnologia, seus dados também estejam contemplados na segurança disposta.

REFERÊNCIAS

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 2 dez. 2022.

CALDEIRA, Cristina. A proteção de Dados Pessoais e o Impacto nas Transferências Internacionais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). *Direito & Internet IV*: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.

CANSIAN, Adriana Cardoso de Moraes. *Aspectos Jurídicos Relevantes da Internet das Coisas (IoT):* Segurança e Proteção de Dados. Adriana Cardoso de Moraes Cansian; orientador Newton De Lucca; Demi Getschko - São Paulo, 2022.

CARLOTO, Selma. *A lei geral de proteção de dados*: enfoque nas relações de trabalho. 2. ed. São Paulo: LTr, 2021.

CNN. *Teen's Tesla hack shows how vulnerable third-party apps may make cars*. Disponível em: <https://edition.cnn.com/2022/02/02/cars/tesla-teen-hack/index.html> Acesso em: 30 jan. 2023.

CYNERIO Research Report. The State of Healthcare IoT Device Security 2022. Acesso em: 29 jan. 2023.

DOHMANN, Idra Spiecker Gen. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *In:* DONEDA, Danilo *et al. Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

DTEC – Grupo de Estudos em Direito e Tecnologia da Universidade Federal de Minas Gerais – UFMG. IoT e Proteção de Dados Pessoais. 23/11/2021. Disponível em: < https://www.dtibr.com/post/iot-e-prote%C3%A7%C3%A3o-de-dados-pessoais> Acesso em: 29 jan. 2023.

EUROACTIV. LEAK: *Commission to introduce cyber requirements for Internet of Things products*. Disponível em: <https://www.euractiv.com/section/cybersecurity/news/leak-commission-to-introduce-cyber-requirements-for-internet-of-things-products/>. Acesso em: 30 jan. 2023.

EUROPEAN Research Cluster on the Internet of Things – IERC. *Internet of Things*. Disponível em:

<http://www.internet-of-things-research.eu/about_iot.htm#:~:text=The%20IERC%20definition%20states%20that,use%20intelligent%20interfaces%2C%20and%20are> Acesso em 29 jan. 2023.

FORBES. *Medical Devices Hit By Ransomware For The First Time In US Hospitals*. Disponível em: <https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/?sh=2486e603425c>. Acesso em: 01 fev. 2023.

GRUPO DE ESTUDOS em Direito e Tecnologia da Universidade Federal de Minas Gerais – DTEC – UFMG. *IoT e Proteção de Dados Pessoais*. 23/11/2021. Disponível em: < https://www.dtibr.com/post/iot-e-prote%C3%A7%C3%A3o-de-dados-pessoais> Acesso em: 29 jan. 2023.

HINTZBERGEN, Jule [et al.]. *Fundamentos de segurança da informação*: com base na ISO 27001 e na ISO 27002; tradução Alan de Sá – Ed. Brasport, Rio de Janeiro, 2018.

IOMT (Internet of Medical Things) or healthcare IoT. TechTarget. Disponível em: https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things#:~:text=Examples%20of%20IoMT%20include%20remote,can%20send%20information%20to%20caregivers.> Acesso em 29 jan. 2023.

IOT ANALYTICS. *Insights Release State of IoT Spring 2022*. Disponível em: https://h9e3r9w2.rocket-cdn.me/wp/wp-content/uploads/2022/05/Insights-Release-State-of-IoT-Spring-2022.pdf. Acesso em: 01 fev. 2023.

JALOPNIK. *Researchers Hacked California's Digital License Plates, Gaining Access to GPS Location and User Info (Update).* Disponível em: <https://jalopnik.com/researchers-hacked-californias-digital-license-plates-1849966295?utm_source=twitter&utm_medium=SocialMarketing&utm_campaign=dlvrit&utm_content=jalopnik> Acesso em 30 jan. 2023.

LEAK: *Commission to introduce cyber requirements for Internet of Things products*. Euroactiv. Disponível em: <https://www.euractiv.com/section/cybersecurity/news/leak-commission-to-introduce-cyber-requirements-for-internet-of-things-products/>. Acesso em 30 jan. 2023.

LGPD: Lei Geral de Proteção de Dados Pessoais comentada / coordenadores Viviane Nóbrega Maldonado e Renato Ópice Blum – 3ª ed. rev., atual. e ampl. – São Paulo, Thomson Reuters Brasil, 2021.

LISSARDY, Gerardo. "Despreparada para a era digital, a democracia está sendo destruída", afirma o guru do "big data". *BBC News Brasil*, 9 abr. 2017. Disponível em: https://www.bbc.com/portuguese/geral-39535650. Acesso em: 28 nov. 2022.

MCKINSEY & COMPANY. *The Internet of Things Catching up to na accelerating opportunity*. Disponível em: <https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf>. Acesso em 01 fev. 2023.

MICROSOFT Digital Defense Report 2022. Disponível em: < https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us>. Acesso em 30 jan. 2023.

MORAES, Alexandre de. *Segurança em IoT*: entendendo os riscos e as ameaças em IoT. Alexandre de Moraes, Victor Takashi Hayashi – Rio de Janeiro, RJ: Alta Books, 2021.

PARENTONI, Leonardo. O Direito ao Esquecimento [Right to Oblivion]. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). *Direito & Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

STATE of XIoT Security. T82 – *The Claroty Research Team*. Disponível em: <https://web-assets.claroty.com/resource-downloads/team82-state-of-xiot-1h-2022-1661181434.pdf> Consultado em 29 jan. 2023.

TECHTARGET. *IoMT (Internet of Medical Things) or healthcare IoT*. Disponível em: https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things#:~:text=Examples%20of%20IoMT%20include%20remote,can%20send%20information%20to%20caregivers.> Acesso em 29 jan. 2023.

THE WORLD'S most valuable resource is no longer oil, but data. *The Economist*, 6 maio 2017. Disponível em: www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 28 nov. 2022.

TOMASEVICIUS FILHO, Eduardo. Inteligência artificial e direitos da personalidade: uma contradição em termos? *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, v. 113, pp. 133-149, 2018. Disponível em: https://www.journals.usp.br/rfdusp/article/view/156553. Acesso em: 3 dez. 2022.

DATIFICAÇÃO EM *WEARABLES* DE SAÚDE E OS RISCOS AOS DADOS PESSOAIS:
QUADRO JURÍDICO E DIRETRIZES DEONTOLÓGICAS PARA O CONSELHO FEDERAL DE MEDICINA

Cristiano Colombo

Pós-Doutor em Direito, Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Doutor e Mestre em Direito, Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul (UFRGS). Professor Permanente do Mestrado Profissional em Direito da Empresa e dos Negócios da UNISINOS; Pesquisador FAPERGS em Projeto: "Inteligência Artificial e Proteção de Dados Pessoais: Diálogos entre princípios da Centralidade do ser Humano e Eticidade rumo à concretização no ordenamento jurídico brasileiro." Membro da Red Iberoamericana de Universidades e Institutos con investigación en Derecho e Informática (RED CIIDDI). E-mail: cristianocolombo@unisinos.br

Maique Barbosa de Souza

Mestre em Direito da Empresa e Negócios pela Universidade do Vale do Rio dos Sinos (UNISINOS). Email: maique.b.souza@gmail.com

Wilson Engelmann

Pós-Doutor em Direito Público-Direitos Humanos, Universidade de Santiago de Compostela, Espanha; Doutor e Mestre em Direito Público, Programa de Pós-Graduação em Direito da Unisinos; Professor e Pesquisador do Programa de Pós-Graduação em Direito - Mestrado e Doutorado - da UNISINOS; Bolsista de Produtividade em Pesquisa do CNPq; Pesquisador FAPERGS em Projeto: "Inteligência Artificial e Proteção de Dados Pessoais: Diálogos entre princípios da Centralidade do ser Humano e Eticidade rumo à concretização no ordenamento jurídico brasileiro.". Membro da Red Iberoamericana de Universidades e Institutos con investigación en Derecho e Informática (RED CIIDDI). E-mail: wengelmann@unisinos.br

DOI: https://doi.org/10.59224/dti5.ch8

Resumo: A pesquisa se volta à regulação na proteção da pessoa humana frente à utilização dos *wearables* para a saúde. O tratamento de dados de saúde, por instrumentos tecnológicos ligados ao corpo humano, oferece riscos e desafios a serem superados. O problema indagou como a observação de um quadro jurídico pode contribuir para a orientação de diretrizes deontológicas ao Conselho de Medicina. No primeiro capítulo, foi tratada a datificação e os riscos no tratamento dos dados. No segundo capítulo, a partir do quadro jurídico, voltou-se às diretrizes para a regulação deontológica. A metodologia foi teórica, bibliográfica e normativa.

Palavras-chave: *Wearables*; Proteção de Dados; Diretrizes Deontológicas; Medicina.

Abstract: *A pesquisa se volta à regulação na proteção da pessoa humana frente à utilização dos wearables para a saúde. O tratamento de dados de saúde, por instrumentos tecnológicos ligados ao corpo humano, oferece riscos e desafios a serem superados. O problema indagou como a observação de um quadro jurídico pode contribuir para a orientação de diretrizes deontológicas ao Conselho de Medicina. No primeiro capítulo, foi tratada a datificação e os riscos no tratamento dos dados. No segundo capítulo, a partir do quadro jurídico, voltou-se às diretrizes para a regulação deontológica. A metodologia foi teórica, bibliográfica e normativa.*

Keywords: *Wearables; Data Protection; Deontological Guidelines; Medicine.*

1. INTRODUÇÃO

O presente estudo versa sobre a possível formulação de um quadro jurídico eficiente para a proteção de dados da pessoa humana, frente à utilização dos wearables na área da saúde, tendo como resultante a implementação de diretrizes deontológicas, nos conselhos profissionais de Medicina. A captação e tratamento de dados sensíveis, mediados por instrumentos tecnológicos, ligados ao corpo humano, estão oferecendo riscos e desafios ainda não completamente compreendidos pelos seus usuários e que merecem ser avaliados, nas interações entre seres humanos e máquinas.

O problema de pesquisa indaga sobre: quais são os elementos para a construção de um *legal framework*, na proteção dos titulares de dados pessoais, quando da utilização de dispositivos de computação vestível, na área de saúde? No primeiro capítulo, debruçar-se-á sobre o processo de datificação do ser humano, aguçado pela

utilização de wearables e, em especial, no que toca aos riscos e violações de direitos à luz da disciplina de tratamento dos dados. No segundo capítulo, foram abordados a relevância da eticidade e princípios de proteção no tratamento de dados, no sentido de esquadrinhar diretrizes deontológicas eficientes, promovendo a proteção adequada ao ser humano de seus dados sensíveis. Buscar-se-á indicar possíveis soluções a partir de fundamentos ético-jurídicos, à luz da centralidade do ser humano, que deve permear as interações cibernéticas frente às novas tecnologias. A metodologia foi de cunho teórico, com base em pareceres da União Europeia e de autoridades de proteção de dados, em nível mundial, bem como a observação de resultados de estudos científicos, que se voltaram aos impactos na proteção de dados de utilizadores de wearables.

2. DATIFICAÇÃO EM *WEARABLES* DE SAÚDE E OS RISCOS AOS DADOS PESSOAIS

2.1. DATIFICAÇÃO EM *WEARABLES* DE SAÚDE

A evolução tecnológica alcançada, no último século, fez com que o processo de análise da sociedade fosse alterado de um modelo baseado em teorias e crenças para outro fundamentado de forma mais específica na análise de dados.[1] A observação dos dados captados dos fenômenos sociais tem proporcionado o rompimento de barreiras ideológicas e crenças históricas, permitindo uma visão algorítmica do contexto social. Igualmente, novas respostas e caminhos possíveis são apresentados para a solução de problemas longevos. Ao propor relações aparentemente estranhas – como a associação entre professores e lutadores de sumô, para demonstrar que a humanidade é mais desonesta do que se imagina em razão de atuar baseada em incentivos momentâneos – Steven Levitt e Stephen Dubner rompem barreiras tradicionais, revelando, a partir da análise de dados e de variáveis aparentemente aleatórias, que o comportamento humano nem sempre atua no sentido de proporcionar o máximo de eficiência[2].

1. HARARI, Yuval Noah. *21 lições para o século 21.* Companhia das Letras, 2018.
2. LEVITT, Steven D.; DUBNER, Stephen J. *Freakonomics:* o lado oculto e inesperado de tudo o que nos afeta. Altacult, 2019.

Igualmente, a característica da ubiquidade presente nos sistemas tecnológicos faz com que a produção de dados seja constante, captados a partir de interações nas redes sociais e plataformas de comunicação como Facebook, Twitter, LinkedIn, YouTube, Gmail e Hotmail, bem como pela utilização de dispositivos que captam e transferem metadados destas interações. Estes dados possuem especial relevância, pois são utilizados para a construção de perfis comportamentais que buscam reproduzir o humano no meio virtual, com suas características e preferências, individualizando-o de todos os demais, projetando seu corpo eletrônico[3] como representação da sua personalidade no meio virtual. O ser humano passa a ter sua individualidade projetada no ambiente virtual, a partir de dados que informa, sendo isto captado por empresas que utilizam tais informações para a produção de novos produtos e serviços que atendam a demandas que sequer tinham noção de que existiam.

Este processo, chamado de datificação (ou dataísmo), consiste na "transformação da ação social em dados on-line quantificados, permitindo assim o monitoramento em tempo real e análise preditiva"[4]. Neste contexto, o ser humano e as ações sociais passam a ser percebidos a partir da análise dos dados que eles produzem, os quais são captados, tratados, e com base no *output* gerado, é possível perceber o comportamento futuro provável a partir da análise das ações passadas. Sob esta perspectiva é que a datificação objetiva a captação de dados em massa para que, de acordo com as informações obtidas, seja possível prever tendências e comportamentos futuros. Consoante referido por Wouter Weerkamp e Maarten de Rijke, ao abordar a busca pela predição do comportamento humano, "não estamos interessados na atividade atual ou anterior das pessoas, mas em seus planos futuros"[5]. Assim, considerando que há uma utilização massiva de dispositivos tecnológicos para as interações

3. COLOMBO, Cristiano; NETO, Eugênio Facchini. Corpo elettronico como vítima em matéria de tratamento de dados pessoais: responsabilidade civil por danos à luz da lei de proteção de dados brasileira e dano estético no mundo digital. *In:* DIREITO, governança e novas tecnologias II. Organização CONPEDI/ UNISINOS. CONPEDI, 2018. Disponível em: http://conpedi.danilolr.info/publicacoes/34q12098/15d3698u/Mw0I37P00cGrmxtJ.pdf. Acesso em: 14 mar. 2023.
4. MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data:* a revolution that will transform how we live, work, and think. John Murray, 2013.
5. WEERKAMP, Wouter; DE RIJKE, Maarten. *Activity prediction:* a Twitter-based exploration. SIGIR 2012 Workshop on Time-aware Information Portland, 2012. Disponível em: https://dare.uva.nl/search?metis.record.id=381106. Acesso em: 14 mar. 2023.

humanas, as comunicações não se dão mais no modo *on-line* ou *off-line*, isoladamente, mas se utilizam da tecnologia como meio, ou seja, como instrumento de viabilização da vida, a qual atualmente é vivida no formato *onlife*[6].

Nessa ambiência, o conceito de internet das coisas (IoT) merece especial atenção em razão de que, para cada interação, o ser humano produz novos dados que são captados e informam empresas que se utilizam destes dados para prever comportamentos e desenvolver produtos com base no conhecimento obtido. Dessa forma, quando se observa a "capacidade que os objetos possuem de se comunicar, reportando informações acerca de seu estado e funcionamento"[7], vemos o poder alcançado pelos dispositivos que prometem resultados em troca dos dados. Em razão dessa promessa, os dados são entregues pelos usuários sem que haja consciência sobre eventual exposição a riscos. Nesse processo, com a fusão da ciência da computação com a biologia, a datificação transforma o processo histórico humano em dados capazes de serem observados[8].

Nos termos do Parecer sob nº 8, de 2014, do então denominado "Grupo de Trabalho do Artigo 29º para a Proteção de Dados", da União Europeia, a Internet das Coisas foi apresentada, principalmente, em três desenvolvimentos específicos: "computação vestível, eu quantificado e domótica".[9] A computação vestível, exemplificada pela utilização de acessórios como relógios e óculos, embarcada com sensores, conta com funcionalidades potencializadas por se ligarem a microfones, câmeras e sensores. Outrossim, vale-se de APIs (*Interface de Programação de Aplicações*), na medida que transmitem os dados coletados a terceiros.[10] A seu turno, o "Eu

6. FLORIDI, Luciano. "Soft ethics and the governance of the digital." *Philosophy & Technology*, v. 31, 2018. Disponível em: https://doi.org/10.1007/s13347-018-0303-9. Acesso em: 14 mar. 2023.
7. PATACA, Campos Calenga. *A internet das coisas: tipologias, protocolos e aplicações. the law, state and telecommunications review.* 2020. Disponível em: https://www.academia.edu/43656536/Nome_do_Estudante_CAMPOS_PATACA_A_INTERNET_DAS_COISAS_Tipologias_Protocolos_e_Aplica%C3%A7%C3%B5es_DOUTORAMENTO_EM_TELECOMUNICA%C3%87%C3%95ES_Honolulu_Hawai_Julho_de_2020. Acesso em: 14 mar. 2023.
8. HARARI, Yuval Noah. *Homo Deus:* uma breve história do amanhã. Companhia das Letras, 2015.
9. UNIÃO EUROPEIA. Comissão Europeia. *Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas.* Grupo de trabalho do artigo 29.º Para a Proteção dos Dados. Adotado em 16 set 2014. Disponível em: wp223_en.pdf (europa.eu). Acesso em: 14 mar. 2023.
10. UNIÃO EUROPEIA. Comissão Europeia. *Parecer 8/2014 sobre os recentes desenvolvimentos na*

quantificado" tem como finalidade registrar dados, no sentido quantitativo e qualitativo, que se ligam a "hábitos" e "estilo de vida", como atividades físicas, níveis de pulsação, ganho de massa corporal, entre outras situações.[11] E por último, a "domótica" que se volta à possibilidade de controlar remotamente os eletrodomésticos de casa (*domus*), ou, ainda, de ambientes de escritório, como acender e apagar as luzes, controlar televisores, fornos, máquinas de lavar, enfim, dispositivos em geral, em face de estarem conectados.[12]

Neste contexto, vibrando entre a computação vestível e o eu quantificado estão os "wearables de saúde", que prometem ajudar as pessoas em diversas atividades relacionadas ao bem-estar e a melhora na qualidade de vida. Desde situações simples, como o auxílio a pacientes para se lembrarem de tomar seus medicamentos, regularmente, até outras mais complexas como o implante de chips para a transformação das sensações, fazem com que os wearables de saúde exerçam influência relevante na vida humana e estejam transformando a relação do humano com os objetos ao seu redor. São dispositivos móveis no formato de pulseiras, relógios, fones auriculares, pingentes ou biossensores que a pessoa veste - ou lhe é implantado - e que prometem ajudá-la em inúmeras atividades do dia a dia, e que tiveram seu crescimento impulsionado pela utilização massiva de novas tecnologias. Entre as características dos "wearables" estão: o apelo visual, com a integração às vestimentas, ao corpo ou ligado a um smartphone, adaptando-se às necessidades do usuário; a complementação às habilidades mentais e/ou físicas de seu utilizador; o custo interessante, diante dos benefícios dele decorrentes; as funcionalidades que se volta a questões pessoais e para tarefas de trabalho; e, a facilidade, quando de sua utilização.[13] Por sua vez,

---

Internet das Coisas. Grupo de trabalho do artigo 29.º Para a Proteção dos Dados. Adotado em 16 set 2014. Disponível em: wp223_en.pdf (europa.eu). Acesso em: 14 mar. 2023.

11. UNIÃO EUROPEIA. Comissão Europeia. *Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas.* Grupo de trabalho do artigo 29.º Para a Proteção dos Dados. Adotado em 16 set 2014. Disponível em: wp223_en.pdf (europa.eu). Acesso em: 14 mar. 2023.
12. UNIÃO EUROPEIA. Comissão Europeia. *Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas.* Grupo de trabalho do artigo 29.º Para a Proteção dos Dados. Adotado em 16 set 2014. Disponível em: wp223_en.pdf (europa.eu). Acesso em 14 mar. 2023.
13. CANADÁ. Office of the Privacy Comissioner of Canada. *Wearable computing.* Group of the Office of the Privacy Comissioner of Canada. Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/. Acesso em 14 mar.

dispositivos também são capazes de coletar dados dos usuários, como o humor, a mobilidade, a condição de saúde, bem como do próprio ambiente onde estão, como a temperatura, imagens, umidade e sons[14], inclusive, vozes de não-usuários.

E, neste fluxo comunicacional, os "wearables de saúde" atuam como integradores da tecnologia na ponta das atividades cotidianas, como instrumento para captação dos dados e formação de modelos de comportamento que proporcionam *output* sob medida para as pessoas, ao mesmo tempo em que alimentam as instituições de dados capazes de as colocarem na vanguarda deste processo tecnológico.

Assim os dados possuem alto valor por serem justamente o verdadeiro produto relevante deste processo, sendo entregues pelos usuários em troca de pequenas respostas que atendam a desejos imediatos. Dessa forma, "o paradigma da datificação desempenha, assim, um papel profundamente ideológico na intersecção entre sociabilidade, pesquisa e comércio – um inextricável nó de funções que têm sido subavaliadas"[15], mas que representam um grande valor quando observada sua capacidade de exercício de poder sobre o corpo e a mente humanos. Nessa perspectiva é que os riscos e desafios regulatórios da utilização de wearables de saúde devem ser analisados.

2.2. RISCOS AOS DADOS PESSOAIS

A utilização massiva de "*wearables* de saúde" promete a prevenção de doenças e a gestão de cuidados de saúde diretamente pelo usuário, com o auxílio na promoção de estilos de vida saudável e produtivo. No entanto, o autocuidado promove uma transformação radical na forma de abordagem da saúde, uma vez que com a integração de sensores nos *wearables*, os quais informam as empresas desenvolvedoras com

2023.

14. CANADÁ. Office of the Privacy Comissioner of Canada. *Wearable computing.* Group of the Office of the Privacy Comissioner of Canada. Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/. Acesso em 14 mar. 2023.
15. DIJCK, José Van. "Confiamos nos dados? as implicações da datificação para o monitoramento social." *Matrizes,* v. 11, n. 1 jan./abr. 2017. Disponível em: http://dx.doi.org/10.11606/issn.1982-8160.v11i1p39-59. Acesso em: 14 mar. 2023.

dados sensíveis, surgem problemas relacionados à ética, à privacidade e à regulação. Sobretudo, visto que proporcionam formas de coleta mais discretas de vozes e imagens que os dispositivos que contam com câmaras ostensivas, como são os smartphones.[16] Consoante referido por Xiao Liu, Membro do Centro para a Quarta Revolução Industrial do Fórum Econômico Mundial, ao mesmo tempo em que aceleramos o desenvolvimento da internet das coisas, entramos na era da "Internet dos Corpos"[17], onde uma variedade de dispositivos coleta uma enorme quantidade de dados sensíveis relacionados à saúde, os quais carregam consigo inúmeros desafios a serem superados relacionados à ética e à privacidade, que merecem ser discutidos de forma preventiva, ante o potencial de danos que podem causar.

Em razão da sensibilidade dos dados coletados e do poder sobre o corpo e a mente – e consequentemente sobre o futuro do ser humano -, as preocupações sobre privacidade e a necessidade de adoção de instrumentos de transparência aumentam e podem, inclusive, criar resistência na adoção destes mecanismos[18]. Neste contexto, pode estar se formando uma estrutura de desincentivo da evolução tecnológica ante sua incapacidade de efetivamente proteger o usuário em sua privacidade[19]. Talvez, justamente em razão disso é que a indústria se esforça para que os *wearables* estejam cada vez mais integrados na vida cotidiana, para que atuem de forma imperceptível, situação esta que acaba aumentando os riscos de mau uso dos dados, em razão de que o usuário médio pode encontrar dificuldades em estabelecer barreiras para

16. CANADÁ. Office of the Privacy Comissioner of Canada. *Wearable computing.* Group of the Office of the Privacy Comissioner of Canada. Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/. Acesso em 14 mar. 2023.
17. LUI, Xiao. "Tracking how our bodies work could change our lives." *World Economic Forum*, 2020. Disponível em: https://www.weforum.org/agenda/2020/06/internet-of-bodies-covid19-recovery-governance-health-data/. Acesso em: 14 mar. 2023.
18. BECKER, Moritz. Understanding users' health information privacy concerns for health wearables. *Proceedings of the 51st Hawaii International Conference on System Sciences,* 2018. Disponível em: https://www.researchgate.net/publication/323379590_Understanding_Users'_Health_Information_Privacy_Concerns_for_Health_Wearables. Acesso em: 14 mar. 2023.
19. ENGELMANN, Wilson; SOUZA, Maique Barbosa de. "A nova linguagem global: fluência algorítmica como instrumento capaz de proporcionar confiança nos sistemas de inteligência artificial." *Revista de Direito e as Novas Tecnologias*, v. 13, out./dez. 2021.

proteger os dados que são coletados por seus dispositivos vestíveis. Assim, em razão da necessidade de serem educados sobre os riscos a que estão expostos[20], a discussão sobre novas formas de regulação deve sempre ser atuante, a fim de promover instrumentos eficazes de proteção frente aos novos – e de certa forma desconhecidos - riscos a que estão expostos.

Uma das maiores empresas do segmento, a FITBIT, adquirida pelo Google em 2019 e que saltou de 560 mil usuários em 2012 para 31 milhões em 2020[21], adota frases como "os recursos inovadores de que você precisa para uma vida mais saudável, tudo no seu pulso"[22] para criar a sensação de dependência e incentivar a adoção massiva de seus produtos. Por outro lado, já foi observado que "*wearables*" têm a potencialidade de recolher informações desnecessárias e não informam aos proprietários dos dispositivos todos os dados coletados. Igualmente, os usuários estão expostos a ataques hackers em razão de falhas de segurança nos endereços MAC dos dispositivos[23]. Esta situação, por si só, já é suficiente para suscitar relevantes questionamentos sobre a efetiva proteção dos consumidores, uma vez que os *wearables* da empresa possuem informações extremamente relevantes e que podem ser usadas para estabelecer condicionamentos – e até mesmo direcionamentos – de vida, merecendo, assim, melhores instrumentos que atendam aos princípios de proteção de dados, baseados no modelo de proteção *ex ante*[24].

---

20. CILLIERS, Liezel. "Wearable devices in healthcare: privacy and information security issues." *Health Information Management Journal*, 2019. Disponível em: https://pubmed.ncbi.nlm.nih.gov/31146589/. Acesso em: 14 mar. 2023.
21. STATISTA. *Number of active users of Fitbit from 2012 to 2020.* Disponível em: https://www.statista.com/statistics/472600/fitbit-active-users/. Acesso em: 14 mar. 2023.
22. FITBIT. *Smartwatches.* Disponível em: https://www.fitbit.com/global/us/home. Acesso em: 14 mar. 2023.
23. CYR, Britt; HORN, Webb; MIAO,Daniela; SPECTER, Michael. *Security analysis of wearable fitness devices (Fitbit).* Massachusetts Institute of Technology, 2014. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082016/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf. Acesso em: 14 mar. 2023.
24. ZANATTA, Rafael A. F. *Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?* I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017. Disponível em: https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica. Acesso em: 14 mar. 2023.

Situações como esta vêm sendo cada vez mais frequente, sendo noticiado que dados de mais de 61 milhões de usuários de "*wearables*" relacionados ao estilo de vida fitness foram expostos em uma violação massiva de dados em 2021, os quais continham informações como nome e sobrenome, data de nascimento, peso, altura, sexo, localização geográfica, pressão arterial, peso corporal, níveis de sono, glicose, entre outros, e aparentemente direcionavam estes dados para outra empresa, a qual atua no desenvolvimento de produtos para saúde e bem-estar, além de *wearables* médicos[25]. Apesar de a maioria dos vazamentos de dados ter origem externa às empresas (Externa 61%, Interna 39%), por meio de hackers que buscam superar os bloqueios de segurança para acesso aos dados[26], ainda assim, o usuário deve ter por parte das empresas estruturas de segurança que realmente lhes protejam e contribuam para a construção da confiança necessária para a utilização massiva dos "*wearables*". Lembra-se que para fazer frente aos novos riscos de danos coletivos, devem ser adotados instrumentos eficazes antes que a violação aconteça. No mesmo sentido, a incorreta comunicação com o titular dos dados pode elevar o risco de violação de direitos fundamentais em razão justamente da dificuldade que o usuário possui de escolher o nível adequado de compartilhamento que lhe permita absorver o melhor da tecnologia ao mesmo tempo em que preserva sua privacidade. Além disso, os *outputs* gerados pelos dispositivos podem estar equivocados, pois podem resultar de dados incompletos ou enviesados, não sendo, portanto, fiáveis.

Segundo o Grupo de Trabalho do Artigo 29º para a Proteção de Dados, da União Europeia, os principais riscos a existentes são: a) "a falta de controle e assimetria informacional": como os fluxos comunicacionais são realizadas entre objetos e aplicados automaticamente, torna-se difícil aferir o caminho dos dados, sendo tortuosa a sua fiscalização; b) "qualidade do consentimento do utilizador": a similaridade de um relógio comum para um dispositivo com a tecnologia embarcada é grande, havendo, muitas vezes, dificuldade ao usuário compreender suas diferenças, e, mesmo

25. FOWLER, Jeremiah. Report: Fitness Tracker Data Breach Exposed 61 Million Records and User Data Online. *Website Planet,* 2021. Disponível em: https://www.websiteplanet.com/blog/gethealth-leak-report/. Acesso em: 14 mar. 2023.
26. VERIZON. Data breach investigations report. *DBIR Master's Guide,* 2021. Disponível em: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/. Acesso em: 14 mar. 2023.

consentir de forma adequada com o tratamento de seus dados pessoais. Acrescenta-se que, em alguns casos, existem possibilidades oferecidas pelos *wearables* para renunciar a determinadas funcionalidades, todavia, confrontam diretamente com a usabilidade do dispositivo, afetando diretamente o campo das escolhas; c) "inferências derivadas" e "redefinição da finalidade do tratamento inicial": quando o titular de dados consente para determinada recolha, no entanto, o dispositivo consegue ir além, extraindo novas informações, como é o caso da utilização de dados de acelerômetro para caminhadas que resulte em inferências ao modo de condução de veículos; d) "Provocação invasiva de padrões de comportamento e definição de perfis": em face da grande quantidade de dados recolhidos, são reunidos dados que permitem formar perfil, coletando gostos, hábitos e atitudes das pessoas; e, por último, e) "limitações ao anonimato": a comunicação de dados entre os dispositivos, com a coleta de dados dos usuários dos *wearables* torna possível a sua "reidentificação", em face de localizadores.[27]

Em estudo denominado "*Quality Assurance of Health Wearables Data: Participatory Workshop on Barriers, Solutions, and Expectations*", junto ao Health and Biomedical Informatics Centre, em Melbourne, foram classificados sete grupos de problemas decorrentes do uso de "*Wearables*". São eles: 1º) quanto ao acesso aos dados gerados pelos pacientes: falta de transparência, ausência de consentimento sobre a coleta e uso continuado de dados pessoais; inexistência de acesso aos dados brutos; vazamento de dados; 2º) quanto à acurácia dos dados: imprecisões em face de coletas por diferentes "*wearables*"; erros no *input* dos dados, seja por ser manual, seja por falhas nos sensores dos dispositivos; impossibilidade de edição de dados; 3º) quanto à completude (qualidade de não haver lapsos na coleta dos dados): falta de acesso à internet; insuficiência de bateria; dados manuais não informados; problemas de sincronização entre dispositivos; omissões deliberadas; disfunções nos dispositivos; 4º) quanto à consistência (diferentes dispositivos coletando dados gerando o mesmo significado): problemas de gerenciamento dos dados e imprecisões pelo uso de diferentes plataformas; 5º) quanto à interpretabilidade de dados: excesso no volume de

27. UNIÃO EUROPEIA. Comissão Europeia. *Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas.* Grupo de trabalho do artigo 29. Para a Proteção dos Dados. Adotado em 16 set 2014. Disponível em: wp223_en.pdf (europa.eu). Acesso em 14 mar. 2023.

dados; ausência do contexto em que se operou a recolha, diante dos dados efetivamente coletados; a forma de apresentação de dados por diferentes plataformas; 6º) quanto à relevância dos dados: diferentes julgamentos sobre a importância dos dados; cibercondria, que é a consulta em sites sobre as condições de saúde, na linha da automedicação; 7º) quanto à tempestividade: questões voltadas à disponibilidade de dados, pela demora, na atualização dos mesmos, bem como pela demora que acarreta em dados não estarem filtrados, embora já coletados.[28]

Apesar disso, alguns dispositivos já tiveram sua aprovação confirmada pela Agência Nacional de Vigilância Sanitária do Brasil (Anvisa), a qual por meio da Resolução (RE) 1.635/2020 liberou o Recurso de Notificação de Ritmo Irregular (RNRI) e o eletrocardiograma (ECG) do Apple Watch para aferição de frequência cardíaca em caráter informativo[29]. Ainda que seja necessária a interpretação dos dados pelo médico, a aprovação de um *wearable* como instrumento de monitoramento da saúde denota a aceitabilidade deste tipo de dispositivo por órgãos de controle, bem como revela a tendência de que venham a ser incorporados de forma massiva pela população. Segundo Klaus Schwab, a "tecnologia vestível" tem, como um dos impactos positivos para a saúde, a promoção de "[...] uma vida mais longa"; já na parte dos impactos negativos: "[...] privacidade/potencial vigilância; escapismo e vício; segurança de dados".[30]

Nesse sentido, "com o maior desenvolvimento e aceitação de dispositivos vestíveis", sendo "onipresentes nos níveis organizacional e comunitário"[31], torna-se necessário que sua utilização se opere de forma transparente, ética e segura, com a promoção de um ambiente de confiança e adequação à legislação. Por isso, a falta de

28. ABDOLKHANI, Robab; GREY, Kethleen; BORDA, Ann; SOUZA, Ruth. "Quality assurance of health wearables data: participatory workshop on barriers, solutions, and expectations." *JMIR Mhealth Uhealth* v. 8, n. 1, 2020. e15329. doi: 10.2196/15329 Disponível em: https://mhealth.jmir.org/2020/1/e15329/. Acesso em: 14 mar. 2023.

29. BRASIL. *Resolução-RE nº 1.635.* Agência Nacional de Vigilância Sanitária, 2020. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-re-n-1.635-de-21-de-maio-de-2020-258257094. Acesso em: 14 mar. 2023.

30. SCHWAB, Klaus. *A quarta revolução industrial.* EDIPRO, 2016. p. 121.

31. LI, Caining. LIN, Sapphire H. CHIB, Arul. "The state of wearable health technologies: a transdisciplinary literature review." *Mobile Media & Communication,* 2019. Disponível em: https://journals.sagepub.com/doi/10.1177/2050157920966023. Acesso em: 14 mar. 2023.

controle dos dados e a assimetria informacional do consumidor frente aos riscos que as novas tecnologias impõem, são os principais fundamentos para o estabelecimento de proteção pelas empresas para que a utilização dos "*wearables* de saúde" se dê de forma adequada tanto do ponto de vista jurídico, quanto do ponto de vista dos efeitos ou impactos sociais danosos que pode causar.

3. QUADRO JURÍDICO E DIRETRIZES DEONTOLÓGICOS PARA O CONSELHO FEDERAL DE MEDICINA

O quadro tecnológico apresentado até o momento, desafia o Direito. Se observa uma mudança paradigmática: até algum tempo atrás, somente se admitiria o desenvolvimento de dispositivos vestíveis, que é o caso deste estudo, após o conhecimento dos eventuais riscos. O uso crescente de mecanismos vestíveis, promovendo uma "invasão e coleta" de dados dos usuários, está sendo implementado imediatamente. Isso é uma característica da convergência tecnológica promovida no cenário da Quarta Revolução Industrial. Vale dizer: "o tempo da tecnologia" está em descompasso com o "tempo do Direito".

3.1. QUADRO JURÍDICO

A utilização massiva de dispositivos ligados ao corpo humano com o fito de melhorá-lo a partir de respostas obtidas tende a ser cada vez mais presente. Igualmente, os riscos observados na captação e tratamento dos dados na utilização de *wearables* de saúde, demandam que haja observância de uma estrutura regulatória que estabeleça proteção eficiente desde a construção dos dispositivos, até sua utilização diária.

Assim, uma abordagem ética deve ser presente, fundamentada no respeito à dignidade da pessoa humana, na centralidade no ser humano, bem como no devido cumprimento dos direitos humanos e liberdades fundamentais. Neste contexto, o oferecimento e comercialização de *wearables* relacionados à saúde deve respeitar, minimamente, aos princípios dispostos na Declaração Universal sobre Bioética e Direitos Humanos, em especial o da Dignidade Humana, do Benefício, da Autonomia e Responsabilidade Individual, do Consentimento, do Respeito pela Vulnerabilidade Humana e pela Integridade Individual, da Privacidade, da Confidencialidade, da

Igualdade, Justiça e Equidade, da Não-Discriminação e Não-Estigmatização, da Solidariedade e da Cooperação, do Compartilhamento de Benefícios, da Proteção das Gerações Futuras e do Meio Ambiente[32].

Estes princípios encontram ressonância em outro, específico das novas relações de tratamento de dados por meio da tecnologia, que deve ser somado e que, de certa forma, permeia a todos os anteriores, qual seja o da precaução, pois impõe um limite no agir em cada fase do processo de fabricação e utilização de "*wearables* em saúde", uma vez que obriga as empresas e os reguladores a pensar previamente nos possíveis prejuízos que seus produtos podem ocasionar, colocando em pauta o estabelecimento de freios necessários ao desenvolvimento direcionado para o bem estar humano. Dessa forma, o desenvolvimento dos "*wearables*", assim como da própria inteligência artificial, deve ser centrado no ser humano[33], uma vez que o limite tolerável para os "*wearables* de saúde" é justamente aquele que, mais do que somente proporcionar benefícios, não provoca malefícios ao ser humano, pois não basta fazer o bem, sendo necessário evitar o mal[34].

Outrossim, cumpre destacar a evolução da disciplina de proteção de dados pessoais, em nível mundial. Na União Europeia, a aplicação de um sistema multinível, com a harmonização de legislações dos países membros e do Direito Comunitário, mais especificamente, com a construção do Regulamento Geral de Proteção de Dados Pessoais 2016/679, em substituição à Diretiva 95/46, promovendo tratamento homogêneo, sem "intermediação legislativa", e, de forma "completa e imediata"[35]. O mencionado regulamento significa o divisor de águas de uma forma de tratar os dados sob a perspectiva de um "sistema binário e estático", que se preocupava somente

32. UNESCO. *Declaração Universal sobre Bioética e Direitos Humanos.* Paris, 2006. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000146180_por. Acesso em: 14 mar. 2023.
33. BRAVO, Álvaro Avelino Sánchez. Marco Europeo para una inteligencia artificial basada en las personas. *International Journal of Digital Law,* v. 1, n. 1, jan./abr. 2020. p. 65-78. Disponível em: https://journal.nuped.com.br/index.php/revista/issue/view/vol1n1. Acesso em: 14 mar. 2023.
34. ADAMS, David P.; MILES, Toni P. "The Application of Belmont Report Principles to Policy Development." *Journal of Gerontological Nursing,* v. 39, n. 12, 2013. p. 16-21. Disponível em: 10.3928/00989134-20131028-07. Acesso em: 14 mar. 2023.
35. COLAPIETRO, Carlo. Il diritto alla protezione dei dati personali. in: UN SISTEMA delle fonti multilivello. Scientifica, 2018. p. 24.

com a interação entre titular dos dados e prestador do serviço, para uma proposta multidirecional, em um mundo de plataformas e redes sociais, em que ganha importância o controle dos dados pela pessoa humana.[36] Por sua vez, no Brasil, com o advento da Lei Geral de Proteção de Dados Pessoais, sob o nº 13.709 de 2018, definições, institutos e princípios foram positivados e passaram a orientar a disciplina de proteção de dados pessoais. Em seu artigo 5º, inciso II, estão definidos os dados pessoais sensíveis, assim compreendidos os dados de saúde, visto poderem ser utilizados com maior potencial discriminatório. O artigo 6º dispõe acerca de sua base principiológica, aqui, como destaque: o princípio da finalidade, devendo o dado pessoal sempre ser utilizado de forma compatível com o propósito de sua coleta; da necessidade: não devendo o controlador ou operador de dados ir além dos dados necessários e proporcionais ao serviço que está prestando; da transparência: trazendo informações claras, precisas e de fácil acesso aos usuários; da não-discriminação: comprometendo-se a não utilizar os dados pessoais que teve acesso para injustamente ofertar tratamento diferenciado aos seus usuários, como práticas de *geo-blocking* e *geopricing*. Outrossim, em seu artigo 11, estabelece as hipóteses de tratamento de dados pessoais sensíveis, partindo do consentimento, que deve ser específico e destacado, e, para finalidades específicas, para situações envolvendo cumprimento de obrigações contratuais e regulatórias, políticas públicas e pesquisas, exemplificativamente. Importa destacar que para o tratamento de dados pessoais, no mínimo, uma das hipóteses deverá estar contemplada.

Ademais, ainda que haja o consentimento específico, requisito expresso nas principais legislações de proteção de dados[37], é relevante ter em mente que "nem tudo o que é tecnicamente possível é, de fato, também juridicamente lícito e eticamente admissível, porque não podemos fazer tudo o que é possível fazer"[38]. Isto porque apesar

36. COLAPIETRO, Carlo. Il diritto alla protezione dei dati personali. in: UN SISTEMA delle fonti multilivello. Scientifica, 2018. p. 24.

37. SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. "O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana." *Revista Eletrônica de Direito Civil,* v. 8, n. 1, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 14 mar. 2023.

38. STANZIONE, Pasquale. *Privacy e neurodiritti: la persona al tempo delle neuroscienze.* Giornata

de a união de novas tecnologias com a biologia propor o rompimento de barreiras com a expansão das possibilidades, deve-se sempre observar o limite ético para a preservação do ser humano e do meio ambiente social. A adoção do comportamento ético serve, até mesmo, para o fomento do desenvolvimento tecnológico, pois promove confiança, tanto nos usuários quanto para os reguladores. Dessa forma, a abordagem sob a perspectiva ética ajuda a mitigar o risco que, não é somente pelo compartilhamento dos dados, mas está ligado à legitimidade e à admissibilidade ética de uma intervenção de terceiros no corpo e mente humanos. Assim, a utilização de um dispositivo que alcança tamanho poder sobre o ser humano, merece ter uma interferência percorrida pela ética.

Entre as soluções possíveis e práticas sugeridas pelo Health and Biomedical Informatics Centre estão: 1º) quanto ao acesso aos dados gerados pelos pacientes: considerar a privacidade e a proteção de dados dos titulares, quando do desenho do dispositivo; desenvolver diferentes camadas de consentimento; estabelecer consentimentos dinâmicos; 2º) quanto à acurácia dos dados: estabelecer níveis elevados de mensuração por parte dos fabricantes, inclusive, proporcionando feedbacks aos consumidores, para que identifiquem inexatidões; permitir a ativação de funcionalidade como a edição de dados, nas plataformas dos *wearables*; 3º) quanto à completude: notificar o titular da perda de dados ou de sua coleta, bem como estabelecendo engajamento e educação aos titulares de dados; 4º) quanto à consistência: desenvolver mecanismos para avaliação de fluxo de dados, bem como de verificação, quando a coleta é feita por múltiplos dispositivos; 5º) quanto à interpretabilidade de dados: buscar compreender o contexto em que os dados pessoais são coletados, com a padronização na apresentação dos dados; 6º) quanto à relevância dos dados: desenvolver a literacia, que é a capacidade de ler e interpretar os textos disponíveis na rede mundial de computadores, e, no caso, a combater a cibercondria[39]; 7º) quanto à tempestividade: estabelecer automação e inteligência artificial, para que os dados sejam

europea della protezione dei dati 2021. Disponível em: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9529600. Acesso em: 14 mar. 2023.

39. PISA.21st-Century Readers *Developing literacy skills in a digital world more* info: https://doi.org/10.1787/a83d84cb-en - OCDE. Disponível em: https://read.oecd-ilibrary.org/education/21st-century-readers_a83d84cb-en#page1. Acesso em 14 mar. 2023.

mais rapidamente filtrados e estejam disponíveis. [40]

Lembra-se, mais uma vez, que o desenvolvimento tecnológico não é um fim em si mesmo, mas deve servir de instrumento para proporcionar a melhora do bem-estar ao ser humano e que, para a construção de um ambiente de confiança capaz de alcançar este objetivo, deve-se observar o respeito dos princípios éticos como condição norteadora deste processo[41]. Como visto, "o dataísmo envolve também a confiança nos agentes (institucionais) que coletam, interpretam e compartilham os (meta)dados extraídos da mídia social, das plataformas da internet e outras tecnologias de comunicação"[42], o que revela a necessidade de uma abordagem baseada na ética para o tratamento dos dados operados pelos "*wearables* de saúde".

Luciano Floridi e Mariarosaria Taddeo chamam esse panorama de "ética digital", que está estruturada a partir de três linhas de pesquisa: "a ética dos dados; a ética dos algoritmos e a ética das práticas".[43] Cada uma dessas linhas de pesquisa poderá auxiliar na estruturação das Diretrizes Deontológicas a seguir projetadas, pois o seu objetivo é formular e apoiar moralmente as boas soluções, destacando certos princípios ou condutas ou alguns valores a serem seguidos nos avanços dos dispositivos vestíveis. Se destacam a "confiança" e a "transparência" como dois princípios ou vetores estruturantes da "ética digital". Chama a atenção o que os autores sublinham: "[...] a ética dos dados precisa ser desenvolvida desde o início como uma macroética, ou seja, como uma 'geometria' global do espaço ético, evitando abordagens estreitas e *ad hoc* para versar sobre o conjunto diversificado de implicações éticas provocadas pela

40. ABDOLKHANI, Robab; GREY, Kethleen; BORDA, Ann; SOUZA, Ruth. "Quality assurance of health wearables data: participatory workshop on barriers, solutions, and expectations." *JMIR Mhealth Uhealth* v. 8, n. 1, 2020. e15329. doi: 10.2196/15329 Disponível em: https://mhealth.jmir.org/2020/1/e15329. Acesso em 14 mar. 2023.

41. COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. *Aumentar a confiança numa inteligência artificial centrada no ser humano COM/2019/168 final.* Parlamento Europeu, 2019.

42. DIJCK, José Van. "Confiamos nos dados? as implicações da datificação para o monitoramento social." *Matrizes,* v. 11, n. 1 jan./abr. 2017. Disponível em: http://dx.doi.org/10.11606/issn.1982-8160.v11i1p39-59. Acesso em: 14 mar. 2023.

43. FLORIDI, Luciano; TADDEO, Mariarosaria. What is data ethics? *Philosophical Transactions R. Soc. A,* v. 374, 2016. Disponível em: http://dx.doi.org/10.1098/rsta.2016.0360. Acesso em: 14 mar. 2023.

revolução das informações dentro de um quadro coerente, globalizante, inclusivo e multilateral."[44]

Portanto, se tem uma sinalização de que as preocupações éticas deverão ser estruturadas desde uma perspectiva global, respeitando aspectos locais como a coerência jurídica interna e externa dos Estados, promovendo a inclusão de todas as pessoas, a partir de diálogos transversais e multilaterais.

3.2. DIRETRIZES DEONTOLÓGICAS PARA O CONSELHO FEDERAL DE MEDICINA

A temática acerca das novas tecnologias aplicadas à saúde vinha sendo normatizada, deontologicamente, pelo Conselho Federal de Medicina do Brasil, no mínimo, desde o início deste milênio, com a Resolução CFM nº 1.643 de 7 de agosto de 2002.[45] Do contexto de sua publicação, infere-se que sua abordagem se pautava pela excepcionalidade e voltada a situações de emergência. De seus considerandos, despontam elementos que encaminham para um olhar positivo quanto à sua aplicação, advertência quanto ao cuidado com o sigilo, a confidencialidade e a exigência do consentimento prévio, livre e esclarecido do paciente. Seu texto, no entanto, não faz referência a dispositivos aplicados à saúde. Ocorre que, em 6 de fevereiro de 2019, foi publicada a Resolução nº 2.227 de 2018, do Conselho Federal de Medicina, revogando a resolução de 2002. Entre suas disposições, depreende-se pontos interessantíssimos como a determinação para a necessária observância do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, bem como, em seu art. 11, de forma expressa, dispôs sobre "*wearables* de saúde", a saber: "art. 11. O telemonitoramento é o ato realizado sob orientação e supervisão médica para monitoramento ou vigilância a distância de parâmetros de saúde e/ou doença, por meio de aquisição

44. FLORIDI, Luciano; TADDEO, Mariarosaria. What is data ethics? *Philosophical Transactions R. Soc. A,* v. 374, 2016. Disponível em: http://dx.doi.org/10.1098/rsta.2016.0360 Acesso em 14 mar. 2023; e, SCHWAB, Klaus; DAVIS, Nicholas. *Aplicando a quarta revolução industrial*. EDIPRO, 2018. "Suplemento especial: ênfase na ética digital", p. 166.

45. BRASIL. Conselho Federal de Medicina. *Resolução 1.643 de 2002.* Disponível em: https://abmes.org.br/arquivos/legislacoes/Resolucao-CFM-1643-2002-08-07.pdf. Acesso em: 14 mar. 2023.

direta de imagens, sinais e dados de equipamentos e/ou dispositivos agregados ou implantáveis nos pacientes em regime de internação clínica ou domiciliar, em comunidade terapêutica, em instituição de longa permanência de idosos ou no translado de paciente até sua chegada ao estabelecimento de saúde. Parágrafo único. O telemonitoramento inclui a coleta de dados clínicos, sua transmissão, processamento e manejo sem que o paciente precise se deslocar até uma unidade de saúde."[46]

No art. 12, foram estabelecidas as premissas a serem atendidas: "art. 12. No telemonitoramento ou televigilância, as seguintes premissas devem ser atendidas: I - a coordenação do serviço de assistência remota deverá promover o treinamento dos profissionais de saúde locais que intermediarão o atendimento; II - indicação e justificativa de uso da telemedicina assinada pelo médico assistente do paciente; III - garantia de segurança e confidencialidade tanto na transmissão como no recebimento de dados; IV - a transmissão dos dados deve ser realizada sob a responsabilidade do médico encarregado pela assistência regular do paciente; e V - a interpretação dos dados deve ser feita por médico regularmente inscrito no CRM de sua jurisdição e com RQE na área relacionada ao procedimento."[47]

E, na exposição de motivos, assim justificava seus considerandos e determinações: "O impacto da ascensão da telemedicina com o crescente e variável número de aplicativos e dispositivos móveis amigáveis permite que os pacientes usem a tecnologia para monitorar e rastrear sua saúde. Dispositivos de uso doméstico simples, que podem monitorar sinais vitais, permitem a coleta de informações necessárias para diagnóstico por um médico. [...] Os mesmos problemas éticos que podem ser encontrados no atendimento pessoal estão presentes na telemedicina. Se os médicos se concentrarem em manter uma boa relação médico paciente, proteger a privacidade do paciente, promover a equidade no acesso e no tratamento e buscar os melhores resultados possíveis, a telemedicina pode melhorar a prática médica e o cuidado ao paciente. Mesmo sabendo que o conhecimento sobre telemedicina ainda se encontra em evolução, devido ao contínuo aparecimento de tecnologias, o estágio atual já

46. BRASIL. Conselho Federal de Medicina. *Resolução 1.643 de 2002*. Disponível em: https://abmes.org.br/arquivos/legislacoes/Resolucao-CFM-1643-2002-08-07.pdf. Acesso em: 14 mar. 2023.

47. BRASIL. Conselho Federal de Medicina. *Resolução 2.227 de 2018*. Disponível em: https://portal.cfm.org.br/images/PDF/resolucao222718.pdf. Acesso em: 14 mar. 2023.

recomenda a atualização dos atos normativos que estabelecem balizas éticas para suas aplicações."[48]

Portanto, os temas dos dispositivos vestíveis e correlatos foram enfrentados, apontando a necessidade da observância da Ética, bem como da privacidade do paciente. O inusitado foi que, passado exatamente um mês de sua publicação, a Resolução 2.228 de 2019 revogou a resolução de 2018 e restabeleceu a Resolução de 2002, repristinando-a em todos os seus termos.[49] A exposição de motivos da resolução revogadora apontava para inúmeras propostas de alteração normativa, bem como a necessidade de "mais tempo" para reflexão.[50] Em 2020, diante do contexto pandêmico, tanto em nível mundial, como no território brasileiro, a atuação médica foi conduzida às infovias, a merecer orquestração da disciplina de proteção de dados pessoais e de questões de saúde. O Ministério da Saúde brasileiro, por exemplo, nos termos da Portaria 467, permitiu sobre caráter excepcional e temporário a telemedicina, inclusive, para "emitir atestados ou receitas médicas em meio eletrônico"[51].

A boa notícia é que, em 20 de abril de 2022, a temática foi retomada, com a vigente Resolução 2.314, do Conselho Federal de Medicina, que, revogando a resolução de 2002, revisitou a temática, e, em seu artigo 10, parágrafo 2o, dispôs que o "telemonitoramento deve ser realizado por indicação e justificativa do médico assistente do paciente, com garantia de segurança e confidencialidade, tanto na transmissão quanto no recebimento de dados.". Estabeleceu, ainda, que "a transmissão dos dados deve ser realizada sob a responsabilidade técnica da instituição de vinculação do paciente."[52]

48. BRASIL. Conselho Federal de Medicina. *Resolução 2.227 de 2018*. Disponível em: https://portal.cfm.org.br/images/PDF/resolucao222718.pdf. Acesso em: 14 mar. 2023.
49. BRASIL. Conselho Federal de Medicina. *Resolução 2.314 de 2022*. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf. Acesso em: 14 mar. 2023.
50. BRASIL. Conselho Federal de Medicina. *Resolução 2.228 de 2019*. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2019/2228. Acesso em: 2022.
51. BRASIL. *Portaria n.° 467 de 20 de março de 2020.* Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-467-de-20-de-marco-de-2020-249312996. Acesso em: 14 mar. 2023.
52. BRASIL. Conselho Federal de Medicina. *Resolução 1.643 de 2002.* Disponível em: https://abmes.org.br/arquivos/legislacoes/Resolucao-CFM-1643-2002-08-07.pdf. Acesso em: 14 mar. 2023.

Dessa forma, a título colaborativo, em sintonia às linhas apresentadas, compreende-se que os médicos devam comunicar aos seus pacientes riscos e benefícios da utilização de *wearables*, bem como conduzam a sua utilização para dispositivos que contemplem não somente a maior eficácia médica, mas que observem a disciplina de proteção de dados pessoais. Aliás, adverte a exposição de motivos, da Resolução 2.314 do Conselho Federal de Medicina que "no uso da telemedicina impõe uma atualização urgente de atos normativos do CFM", no sentido de "estabelecer balizas éticas", para "a fiscalização, normatização e julgamento do exercício da medicina", conforme competências da Lei 3.268 de 1957.[53]

Nesse sentido, no sentido de colaborar para regulamentação de futuros atos normativos, são apresentadas as seguintes diretrizes:

A uma, o Conselho de Medicina deve fiscalizar e os profissionais devem prescrever o uso de "*wearables*" que estejam em consonância com o direito de privacidade, sem a exposição da vida íntima, bem como em observância ao direito de proteção de dados pessoais, atendendo a Lei Geral de Proteção de Dados. Isto significa que os dados coletados devam estar ligados à finalidade do serviço e funcionalidade do *wearable*, bem como optando pela minimização da recolha, na linha do princípio da necessidade;

A duas, que o *wearable* ao valer-se dos dados coletados, esteja de acordo com as hipóteses de tratamento, e, caso seja pela via do consentimento, atenda ao artigo 11 da Lei Geral de Proteção de Dados Pessoais, que determina seja o consentimento específico e destacado, inclusive, sendo devidamente cientificado o titular dos dados, quanto às hipóteses de compartilhamento, pautadas sempre pela finalidade;

A três, diante da possibilidade de erros, e, sobretudo, em caso de aplicação de decisões automatizadas ou de inteligência artificial, permita o direito à revisão ou à retificação dos dados pessoais pelos pacientes, que possam sofrer as consequências de desatualizações, erros de *input*, entre outros;

A quatro, atenda a segurança da informação, em especial, a cibersegurança, valendo-se de criptografia e serviços de computação em nuvem que protejam os dados

53. BRASIL. Conselho Federal de Medicina. *Resolução 1.643 de 2002*. Disponível em: https://abmes.org.br/arquivos/legislacoes/Resolucao-CFM-1643-2002-08-07.pdf. Acesso em: 14 mar. 2023.

pessoais dos pacientes;

A cinco, prestadores de serviço voltados a *wearables* tenham em sua equipe profissionais da área médica, a revisar os protocolos médicos utilizados como componentes na formação do algoritmo;

A seis, estejam com encarregado de proteção de dados pessoais devidamente identificado, com os canais de comunicação e pronto a responder e cumprir os direitos dos titulares de dados pessoais, nos termos do artigo 18 da LGPD.

A sete, enfim, observem o princípio da eticidade, da centralidade da pessoa humana, da transparência e auditabilidade do sistema e dos procedimentos de coleta e tratamento dos dados.

4. CONSIDERAÇÕES FINAIS

O estudo versou sobre o contexto da datificação e os "*wearables* de saúde", na busca de compor quadro jurídico, tendo como resultante diretrizes ao Conselho Federal de Medicina, do Brasil. Compreende-se, a título de considerações finais, que deva o órgão de classe encaminhar a devida orientação aos seus profissionais, no sentido de tutelar o direito de privacidade e proteção de dados pessoais de seus pacientes, a observar os princípios da LGPD, bem como as hipóteses de tratamentos de dados pessoais, nos termos do artigo 11. As reflexões também apontam medidas concretas, nos veios dos princípios da eticidade e da centralidade da pessoa humana. O acesso aos dados dos pacientes deverá ser tratado como um tema de máxima importância, sempre orientado pelo respeito ao máximo cuidado desse material. A LGPD deverá ser o guia jurídico principal, amparado nas diretrizes acima explicitadas, além de outras que a prática cotidiana possa revelar como fundamental para a estruturação da disciplina "ética digital na área da saúde", no segmento dos dispositivos vestíveis.

REFERÊNCIAS

ABDOLKHANI, Robab; GREY, Kethleen; BORDA, Ann; SOUZA, Ruth. "Quality assurance of health wearables data: participatory workshop on barriers, solutions, and expectations." *JMIR Mhealth Uhealth* v. 8, n. 1, 2020. e15329. doi: 10.2196/15329 Disponível em: https://mhealth.jmir.org/2020/1/e15329/. Acesso em: 14 mar. 2023.

ADAMS, David P.; MILES, Toni P. "The Application of Belmont Report Principles to Policy Development." *Journal of Gerontological Nursing,* v. 39, n. 12, 2013. p. 16-21. Disponível em: 10.3928/00989134-20131028-07. Acesso em: 14 mar. 2023.

BECKER, Moritz. Understanding users' health information privacy concerns for health wearables. *Proceedings of the 51st Hawaii International Conference on System Sciences,* 2018. Disponível em: https://www.researchgate.net/publication/323379590_Understanding_Users'_Health_Information_Privacy_Concerns_for_Health_Wearables. Acesso em: 14 mar. 2023.

BRASIL. Conselho Federal de Medicina. *Resolução 1.643 de 2002.* Disponível em: https://abmes.org.br/arquivos/legislacoes/Resolucao-CFM-1643-2002-08-07.pdf. Acesso em: 14 mar. 2023.

BRASIL. Conselho Federal de Medicina. *Resolução 2.227 de 2018*. Disponível em: https://portal.cfm.org.br/images/PDF/resolucao222718.pdf. Acesso em: 14 mar. 2023.

BRASIL. Conselho Federal de Medicina. *Resolução 2.228 de 2019*. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2019/2228. Acesso em: 14 mar. 2023.

BRASIL. Conselho Federal de Medicina. *Resolução 2.314 de 2022*. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf. Acesso em: 14 mar. 2023.

BRASIL. *Portaria n.° 467 de 20 de março de 2020.* Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-467-de-20-de-marco-de-2020-249312996. Acesso em: 14 mar. 2023.

BRASIL. *Resolução-RE nº 1.635.* Agência Nacional de Vigilância Sanitária, 2020. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-re-n-1.635-de-21-de-maio-de-2020-258257094. Acesso em: 14 mar. 2023.

BRAVO, Álvaro Avelino Sánchez. Marco Europeo para una inteligencia artificial basada en las personas. *International Journal of Digital Law,* v. 1, n. 1, jan./abr. 2020. p. 65-78. Disponível em: https://journal.nuped.com.br/index.php/revista/issue/view/vol1n1. Acesso em: 14 mar. 2023.

CANADÁ. Office of the Privacy Comissioner of Canada. *Wearable computing.* Group of the Office of the Privacy Comissioner of Canada. Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/. Acesso em 14 mar. 2023.

CILLIERS, Liezel. "Wearable devices in healthcare: privacy and information security issues." *Health Information Management Journal*, 2019. Disponível em: https://pubmed.ncbi.nlm.nih.gov/31146589/. Acesso em: 14 mar. 2023.

COLAPIETRO, Carlo. Il diritto alla protezione dei dati personali. in: UN SISTEMA delle fonti multilivello. Scientifica, 2018.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. "Corpo elettronico como vítima em matéria de tratamento de dados pessoais: responsabilidade civil por danos à luz da lei de proteção de dados brasileira e dano estético no mundo digital." in: DIREITO, governança e novas tecnologias II.

Organização CONPEDI/ UNISINOS. CONPEDI, 2018. Disponível em: http://conpedi.danilolr.info/publicacoes/34q12098/15d3698u/Mw0I37P00cGrmxtJ.pdf. Acesso em: 14 mar. 2023.

COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. *Aumentar a confiança numa inteligência artificial centrada no ser humano COM/2019/168 final.* Parlamento Europeu, 2019.

CYR, Britt; HORN, Webb; MIAO, Daniela; SPECTER, Michael. *Security analysis of wearable fitness devices (Fitbit).* Massachusetts Institute of Technology, 2014. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082016/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf. Acesso em: 14 mar. 2023.

DIJCK, José Van. "Confiamos nos dados? as implicações da datificação para o monitoramento social." *Matrizes,* v. 11, n. 1 jan./abr. 2017. Disponível em: http://dx.doi.org/10.11606/issn.1982-8160.v11i1p39-59. Acesso em: 14 mar. 2023.

ENGELMANN, Wilson; SOUZA, Maique Barbosa de. "A nova linguagem global: fluência algorítmica como instrumento capaz de proporcionar confiança nos sistemas de inteligência artificial." *Revista de Direito e as Novas Tecnologias*, v. 13, out./dez. 2021.

FITBIT. *Smartwatches.* Disponível em: https://www.fitbit.com/global/us/home. Acesso em: 14 mar. 2023.

FLORIDI, Luciano. "Soft ethics and the governance of the digital." *Philosophy & Technology*, v. 31, 2018. Disponível em: https://doi.org/10.1007/s13347-018-0303-9. Acesso em: 14 mar. 2023.

FOWLER, Jeremiah. Report: Fitness Tracker Data Breach Exposed 61 Million Records and User Data Online. *Website Planet,* 2021. Disponível em: https://www.websiteplanet.com/blog/gethealth-leak-report/. Acesso em: 14 mar. 2023.

HARARI, Yuval Noah. *Homo Deus:* uma breve história do amanhã. Companhia das Letras, 2015.

HARARI, Yuval Noah. *21 lições para o século 21.* Companhia das Letras, 2018.

LEVITT, Steven D.; DUBNER, Stephen J. *Freakonomics:* o lado oculto e inesperado de tudo o que nos afeta. Alta Cult, 2019.

LI, Caining. LIN, Sapphire H. CHIB, Arul. "The state of wearable health technologies: a transdisciplinary literature review." *Mobile Media & Communication,* 2019. Disponível em: https://journals.sagepub.com/doi/10.1177/2050157920966023. Acesso em: 14 mar. 2023.

LUI, Xiao. "Tracking how our bodies work could change our lives." *World Economic Forum*, 2020. Disponível em: https://www.weforum.org/agenda/2020/06/internet-of-bodies-covid19-recovery-governance-health-data/. Acesso em: 14 mar. 2023.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data:* a revolution that will transform how we live, work, and think. John Murray, 2013.

PATACA, Campos Calenga. *A internet das coisas: tipologias, protocolos e aplicações. the law, state and telecommunications review.* 2020. Disponível em:

https://www.academia.edu/43656536/Nome_do_Estudante_CAMPOS_PATACA_A_INTERNET_DAS_COISAS_Tipologias_Protocolos_e_Aplica%C3%A7%C3%B5es_DOUTORAMENTO_EM_TELECOMUNICA%C3%87%C3%95ES_Honolulu_Hawai_Julho_de_2020. Acesso em: 14 mar. 2023.

PISA.21st-Century Readers *Developing literacy skills in a digital world more* info: https://doi.org/10.1787/a83d84cb-en - OCDE. Disponível em: https://read.oecd-ilibrary.org/education/21st-century-readers_a83d84cb-en#page1. Acesso em 14 mar. 2023.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. "O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana." *Revista Eletrônica de Direito Civil,* v. 8, n. 1, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 14 mar. 2023.

SCHWAB, Klaus. *A quarta revolução industrial.* EDIPRO, 2016.

SCHWAB, Klaus; DAVIS, Nicholas. *Aplicando a quarta revolução industrial.* EDIPRO, 2018. "Suplemento especial: ênfase na ética digital".

STANZIONE, Pasquale. *Privacy e neurodiritti: la persona al tempo delle neuroscienze.* Giornata europea della protezione dei dati 2021. Disponível em: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9529600. Acesso em: 14 mar. 2023.

STATISTA. *Number of active users of Fitbit from 2012 to 2020.* Disponível em: https://www.statista.com/statistics/472600/fitbit-active-users/. Acesso em: 14 mar. 2023.

UNESCO. *Declaração Universal sobre Bioética e Direitos Humanos.* Paris, 2006. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000146180_por. Acesso em: 14 mar. 2023.

UNIÃO EUROPEIA. Comissão Europeia. *Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas.* Grupo de trabalho do artigo 29.º Para a Proteção dos Dados. Adotado em 16 set 2014. Disponível em: wp223_en.pdf (europa.eu). Acesso em 14 mar. 2023.

VERIZON. Data breach investigations report. *DBIR Master's Guide,* 2021. Disponível em: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/. Acesso em: 14 mar. 2023.

WEERKAMP, Wouter; DE RIJKE, Maarten. *Activity prediction:* a Twitter-based exploration. SIGIR 2012 Workshop on Time-aware Information Portland, 2012. Disponível em: https://dare.uva.nl/search?metis.record.id=381106. Acesso em: 14 mar. 2023.

TRANSPARÊNCIA DE DIREITO E TRANSPARÊNCIA DE FATO NO TRATAMENTO DE DADOS PESSOAIS EM IOT:
UM OLHAR SOBRE A APLICAÇÃO DA ISO 31700 E DA ÉTICA SUSTENTÁVEL

Daniela Monte Serrat Cabella

Advogada Especialista em Proteção de Dados e Privacidade. Cofundadora da Complete Privacy.

Dionéia Motta Monte-Serrat

Pesquisadora Colaboradora no Depto. de Computação e Matemática, FFCLRP-USP. Profa. Assistente Doutora na Universidade de Ribeirão Preto, Unaerp. Advogada.

DOI: https://doi.org/10.59224/dti5.ch9

Resumo: Impactos da *IoT* requerem transparência material em relação ao tratamento de dados. A ISO 31700 integra tecnologia, *Privacy by Design* (Cavoukian, 2011), gestão de riscos e a relação mutável e contextual entre usuário e organização. Considerando o aspecto dinâmico da ética sustentável sob a perspectiva relacional, propomos conceito que integra todos esses elementos. Sua prática acelera o desenvolvimento da inovação, viabiliza a sustentabilidade, consistência e confiabilidade à organização, seus produtos e serviços a longo prazo, e evita percalços antiéticos, ausência da transparência de fato e suas consequências.

Palavras-chave: Transparência; *Privacy by Design*; Ética Sustentável.

Abstract: *IoT impacts require material transparency regarding data processing. ISO 31700 integrates technology, Privacy by Design, risk management and the changing, contextual relationship between user and organization. Considering the dynamic aspect of sustainable ethics from a relational perspective, we propose a concept that integrates all these elements. Its practice accelerates the development of innovation, enables sustainability, consistency and reliability for the organization, its products, and services in the long term, and avoids unethical mishaps, lack of transparency and its consequences.*

Keywords: *Transparency. Privacy by Design. Sustainable Ethics.*

Sumário: Introdução; 1. Reflexões sobre o tratamento de dados pessoais em *IoT*; 2.

INTRODUÇÃO

A propagação da inovação tecnológica para casas, carros autônomos, supermercados automatizados, relações de consumo, entre outros, desperta novos debates sobre a comunicação com os usuários de dispositivos cibernéticos. A automação, turbinada pela Internet das Coisas (*Internet of Things, IoT*), que se baseia em conectividade sem fio de banda larga à Internet, faz com que tudo esteja conectado a tudo.

Esse panorama da *IoT* levanta importantes questões quanto aos limites da tutela dos dados pessoais. O fato de reunir o uso de sensores a um conjunto de serviços e dispositivos que promovem conectividade faz com que a *IoT* envolva o tratamento de dados pessoais de forma contínua, restando, portanto, intimamente ligada ao ser humano. Essa integração entre pessoas e tecnologias decorre: i) do estado de disponibilidade para se comunicar a qualquer momento (*always-on*) ou da acessibilidade (*ready access*); ii) da quantidade de informações, da interatividade e do armazenamento ininterrupto de dados (*always recording*) (Magrani, 2018).

Objetos com sensores e outras tecnologias estão à disposição em todo lugar e a qualquer tempo, permitindo ao usuário que se conecte a eles para realizar um monitoramento das condições atuais de saúde, um monitoramento remoto de um ambiente ou para concretizar relação de consumo, por exemplo. Embora os sistemas tecnológicos se entrelacem à normalidade da inovação para gerenciar coisas e facilitar decisões do indivíduo no dia a dia, não se pode esquecer de que eles ocultam um paradoxo: o dispositivo, ao mesmo tempo em que pode proteger ou facilitar a vida do usuário, pode também, de certa forma, controlar seu comportamento sem que esse usuário se dê conta desse fato.

A *IoT* não deve ser compreendida somente sob uma ótica descentrada e abstrata.

Ela deve também ser analisada quanto aos impactos sobre a subjetividade do usuário – daí a necessidade de proteção dos dados deste último. O acúmulo de informação sobre o indivíduo em uma relação de consumo, por exemplo, o fragiliza diante de organizações cujos objetivos não restam muito claros. Decisões da parte mais forte nessa relação (organização) podem ser tomadas a partir da conectividade com a *IoT*, alcançando meios para disciplinar o usuário ou tirá-lo das condições em que se encontra (Monte-Serrat, 2021; Monte-Serrat e Cattani, 2022). Essa situação envolve uma complexidade que vai além das regulamentações legais e põe em xeque princípios éticos de maneira a dificultar seriamente a aplicação deles para o futuro. A relação homem-tecnologia, por mais que seja regulada, precisa ser algo que se sustente e produza reflexos positivos para o futuro, inclusive éticos, em relação à privacidade.

Nesse sentido, o presente Capítulo destaca que a realidade vivenciada pelo usuário de dispositivos de *IoT*, nas relações de consumo, pode ser muito diferente daquilo que preconiza a lei. Isso configura um descompasso entre a realidade vivenciada pelo consumidor e os estatutos legais disciplinadores dessa realidade. Por mais que os produtos e serviços inovadores sigam a legislação de proteção de dados do usuário, ainda podem ocorrer situações antiéticas. O que estaria faltando para que haja sincronia entre a inovação e as práticas éticas efetivas?

Sugerimos, ainda, um dos caminhos para alcançar uma inovação responsável na atualidade e que também traga responsabilidade em relação ao futuro. Trazemos o novo conceito de *Tripé da Aceleração da Inovação* (Cabella, 2022) para analisar a comunicação com usuários de dispositivos de *IoT* à luz da ISO 31700 (2023). Mostramos que a aplicação do conceito de ética sustentável (Cabella e Monte-Serrat, 2022) por meio do *framework* de *Privacy by Design* (Cavoukian, 2011) consolida-se em norma de aplicação global (ISO 31700-1 e ISO/TR 31700-2) (2023), o que configura uma forma de garantir a sustentabilidade tanto de produtos e serviços de *IoT*, como também da própria organização que os oferta.

Em resumo, a vulnerabilidade do usuário verificada nas relações de consumo requer uma abordagem de múltiplos elementos. Nossa proposta é de que a privacidade seja gerenciada desde a concepção do dispositivo e serviços de *IoT* e acompanhe as alterações no produto, serviço ou no contexto da organização. Isso torna a inovação sustentável e ética, o que vai muito além da adequação às leis e regulamentos existentes no Brasil. Organizações que adotem essa estratégia estarão capacitadas a

aproveitar as promessas tecnológicas de maneira a inspirar confiança ao usuário de que seus direitos serão respeitados e sua privacidade estará protegida tanto na atualidade como no futuro.

1. REFLEXÕES SOBRE O TRATAMENTO DE DADOS PESSOAIS EM IOT

Uma visão ingênua sobre a Internet da Coisas (*IoT*) traz deslumbramento ao indivíduo que, através do uso da tecnologia, torna-se apto a conectar objetos de sua vida cotidiana (como eletrodomésticos, carro, aparelhos de som, televisão etc.) à internet para que haja comunicação entre ele e esses objetos. Muitas vantagens são oferecidas pelas organizações que, através de seus produtos, têm acesso direto à gravação, monitoramento e ajustes da interação entre o usuário do produto e os itens conectados. Muitas facilidades são trazidas ao indivíduo na forma de benefícios. No entanto, o usuário hiperconectado não se dá conta de que pode haver um movimento intencional, e pouco notado, de violação de sua privacidade em favor da organização que grava, monitora e ajusta esses dados.

Zuboff (2019) traz um alerta importante em relação ao tratamento massivo de dados pessoais, dizendo que muitas organizações conseguem, com ele, praticamente prever ações dos usuários, e manipulá-los ou vender essas informações sem que os usuários tenham qualquer ciência disso. Em nosso entendimento, muito além da falta de transparência e consequente assimetria de informação, que são ilegais e devem ser corrigidas, há questões operacionais na criação, desenvolvimento e implementação da inovação, bem como decisões de risco tomadas nesse processo que devem ser analisadas com cuidado. Embora esses elementos possam estar em conformidade com a legislação, ao mesmo tempo podem configurar, paradoxalmente, situações antiéticas e não sustentáveis a longo prazo. Esse fato pode gerar questionamentos por parte de clientes e parceiros comerciais e investigações de autoridades públicas com impactos severos à operação, reputação e saúde financeira da organização. Nesse cenário, contratos importantes podem ser rescindidos e a confiança dos usuários consumidores pode ser quebrada.

Um impacto negativo como esse pode dar ensejo à derrocada da organização. Esse é um dos motivos pelos quais é muito importante garantir que a inovação (com destaque para a *IoT*) seja desenvolvida de forma sustentável.

Outra questão complexa envolvendo o tratamento de dados por dispositivos e serviços de *IoT* é a sua característica dinâmica, própria da inovação. As mudanças no mundo fático tecnológico ocorrem antes mesmo que leis e regulamentos surjam ou sejam atualizados, e muito antes que decisões judiciais modulem a aplicação legal. Em outras palavras, os legisladores, os reguladores e o judiciário estão sempre a *um passo atrás* da inovação. Essa é mais uma justificativa para que as organizações adotem uma estratégia igualmente dinâmica no tratamento de dados, a fim de garantir sustentabilidade própria e de seus produtos e serviços de *IoT* a longo prazo.

2. TRANSPARÊNCIA NA COMUNICAÇÃO COM O USUÁRIO NO CONTEXTO DO TRATAMENTO DE DADOS

Um fundamento para que a sustentabilidade seja atingida é a garantia de *transparência* na comunicação com o usuário em relação ao tratamento de seus dados pessoais.

Paal e Pauly (2018) comentam que a transparência tem elementos prospectivos e retrospectivos. O prospectivo se refere à situação em que os indivíduos devem ser informados sobre o processamento de dados em andamento antes que esse processamento ocorra. Isso exige que os controladores de dados informem aos seus titulares quem processa os dados, o por quê e para quê esse processamento é feito. Isso deve ser feito através do uso de linguagem acessível e fácil de entender. O elemento retrospectivo relaciona-se à possibilidade de rastreamento do como e do por quê uma determinada decisão foi tomada em relação ao tratamento de dados pessoais.

A aplicação do princípio da transparência ao processamento de informações pessoais existe pelo menos desde 1973, quando o Comitê de Sistemas Automatizados de Dados Pessoais do Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos criou e recomendou a aplicação do *Code of Fair Information Practice – CFIP* (1973). Posteriormente, deu origem aos atualmente chamados de Princípios da Prática Justa da Informação (*Fair Information Practice Principles – FIPPs*). Esse Código define o que seria o básico de práticas consideradas como justas aplicáveis ao tratamento de dados pessoais – o mínimo que toda organização com esse tipo de atividade deveria aplicar.

É interessante notar que, já naquela época, antes da criação do primeiro

dispositivo de *IoT*[1] de que se tem notícia, havia a preocupação com os reflexos do processamento de dados pessoais por meio da tecnologia na privacidade dos indivíduos. O Relatório que propôs o *CFIP* (1973) assinala que, "embora não haja nada inerentemente injusto em trocar alguma medida de privacidade por um benefício, ambas as partes da troca devem participar da definição dos termos" (tradução livre). Também traz o seguinte destaque: "de acordo com a lei atual, a privacidade de uma pessoa é pouco protegida contra práticas arbitrárias ou abusivas de manutenção de registros" *CFIP* (1973) (tradução livre) – observação essa que, infelizmente, ainda reflete a realidade dos dias de hoje.

Um dos princípios sobre os quais o *CFIP* (1973) se baseia é o da transparência, nos seguintes termos: "Deve haver uma maneira de um indivíduo descobrir quais informações sobre ele estão em um registro e como elas são usadas" nos sistemas automatizados (tradução livre). Segundo o Código, uma prática que não atendesse a esse princípio seria considerada "desleal" e estaria sujeita a penalidades criminais e recursos civis.

A redação do princípio da transparência dentro do contexto dos *Fair Information Practice Principles, FIPPs* (2023) evoluiu e, na atualidade, ele é descrito do seguinte modo: "Transparência. As agências devem ser transparentes sobre as políticas e práticas de informação com relação a PII e devem fornecer avisos claros e acessíveis sobre criação, coleta, uso, processamento, armazenamento, manutenção, disseminação e revelação de PII." (tradução livre).

Na Europa, vale lembrar que a Diretiva 95/46/EC do Parlamento Europeu e do Conselho da União Europeia determinava que o processamento de dados pessoais fosse feito de maneira lícita e leal, e que as finalidades do tratamento deveriam ser explícitas. No entanto, somente com o Regulamento (GDPR) 2016/679 também chamado de Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* – GDPR, 2016), é que a transparência foi consolidada explicitamente como um princípio e um direito do titular de dados com aplicação transnacional.

1. O que só veio a ocorrer na década de 1980, com uma máquina de Coca-Cola que foi adaptada por David Nichols para reportar seu conteúdo por meio de uma rede (fonte: Teicher, J. (2018). *The little-known story of the first IoT device*. IBM Blog, 7 de fevereiro de 2018. Acesso em 26 de março de 2023. Retirado de https://www.ibm.com/blog/little-known-story-first-iot-device/).

No cenário brasileiro, por sua vez, a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais – LGPD (Brasil, 2018), que tem a inovação como fundamento expresso da disciplina da proteção de dados pessoais (art. 2º, inciso V), estabelece que o tratamento destes últimos deverá observar a boa-fé e a transparência, garantindo a disponibilização, aos titulares, de "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento" (art. 6º, *caput* e inciso VI). No art. 9º, reforça-se a transparência pela determinação de que o acesso a essas informações seja "facilitado" e de que elas sejam disponibilizadas "de forma clara, adequada e ostensiva".

Além da LGPD (Brasil, 2018), outras leis anteriores já estabeleceram importantes previsões acerca da transparência em relação ao tratamento de dados pessoais e nas relações de consumo. O art. 11, §3º, da Lei nº 12.965/2014, Marco Civil da Internet – MCI, (Brasil, 2014), por exemplo, estipula que os provedores de conexão e de aplicação de internet devem disponibilizar informações sobre o tratamento de dados pessoais. A ausência dessas informações será considerada uma infração e está sujeita às penalidades previstas no art. 12[2], sem prejuízo de outras sanções cabíveis.

No que diz respeito especificamente ao âmbito da relação de consumo, a Lei nº 8.078/1990 (Brasil, 1990), ou Código de Defesa do Consumidor, CDC, estabeleceu como direito básico do consumidor a informação adequada e clara sobre os produtos e serviços e sobre os riscos que apresentem[3] (art. 6º, inciso III) – o que, em nosso entendimento, também envolve o aspecto do tratamento de dados pessoais, quando presente, por ser essencial ao produto ou serviço. Além disso, informações insuficientes ou inadequadas sobre a utilização de produtos e fruição de serviços e os riscos envolvidos dão ensejo à responsabilidade civil, conforme previsões da Seção II do

2. Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
3. É interessante notar que, em 2015, acrescentou-se a exigência de acessibilidade da informação com a previsão do parágrafo único3 do art. 6º, especificamente voltado para a pessoa com deficiência.

Capítulo IV do CDC (Brasil, 1990).

Do art. 31 do mesmo Código (Brasil, 1990), é possível depreender que, na apresentação de serviços ou produtos (inclusive de *IoT*) que envolvam o tratamento de dados pessoais, devem ser fornecidas informações "corretas, claras, precisas, ostensivas e em língua portuguesa" sobre suas características e sobre os riscos que geram aos consumidores. Vale ressaltar que qualquer tipo de comunicação de caráter publicitário que omita informações essenciais sobre o produto ou serviço, ou seja total ou parcialmente falsa, ou, de qualquer outra forma possa induzir em erro o consumidor, será considerada enganosa (art. 37, §§ 1º e 3º, e art. 66, CDC) (Brasil, 1990). E ainda, se a comunicação tirar proveito da ignorância do consumidor, considerando-se sua idade ou [falta de] conhecimento, poderá configurar prática abusiva e expressamente vedada nos termos do art. 39 do CDC (Brasil, 1990).

O art. 43 (Brasil, 1990) determina, expressamente, que seja dado ao consumidor "acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes" (*caput*) e que os cadastros e dados desse titular de dados "devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão" (§ 1º)[4] (Brasil, 1990). Impedir ou dificultar, de qualquer modo, o acesso a essas informações constitui infração penal com pena de detenção ou multa (art. 72) (Brasil, 1990).

Por fim, destacamos que as condições contratuais de uma prestação de serviços ou da compra de um produto (inclusive de *IoT*) que "estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a equidade" (art. 51, *caput* e inciso IV) (Brasil, 1990) são consideradas abusivas e nulas de pleno direito. Essa previsão também pode ser aplicável às cláusulas referentes ao tratamento de dados pessoais na relação de consumo.

Em resumo, podemos observar que, pelo menos desde a década de 1970, o princípio da transparência tem sido adotado por diversas diretrizes, leis e regulamentos ao redor do mundo. No entanto, permanece a dificuldade em determinar qual o nível de detalhe que uma explicação *significativa* deve alcançar. Os autores (Felzmann et

4. Em 2015, acrescentou-se o § 6º com a previsão de que todas essas informações devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência.

al., 2019) declaram que a necessidade de transparência na interação humano-tecnologia deve estar atrelada a requisitos necessários à sua implantação, evitando, assim armadilhas e obstáculos. Eles chegam ao consenso de que ainda não há resultados claros com relação aos benefícios da transparência para usuários de tecnologias inovadoras, como a inteligência artificial e os dispositivos de *IoT*, justamente por haver interferência de uma ampla gama de *fatores contextuais*. Esse estudo (Felzmann et al., 2019) mostra, portanto, que a transparência exigida pela lei pode ser insuficiente, e que há a necessidade de entendê-la sob uma forma *relacional*. Em outras palavras, a *comunicação* entre fornecedores de produtos e serviços de tecnologia e usuários consumidores deve ter a confiabilidade baseada em fatores contextuais.

3. POR UMA TRANSPARÊNCIA QUE ENTRELACE FATO E DIREITO

A inovação tecnológica torna cada vez mais complexa a tomada de decisão pelas organizações em relação ao tratamento de dados pessoais, bem como a implantação da transparência jurídica imposta pela legislação. O desafio está em tornar o usuário consumidor de produtos e serviços de tecnologia, que se relaciona com a organização que os fornece, ciente dos termos, condições e riscos ligados ao tratamento de seus dados pessoais, de quais são seus direitos e como pode exercê-los e capaz de ter acesso a essas informações que impactam sua vida e decisões.

De outro modo, podemos dizer que a transparência na proteção de dados é um princípio fundamental a ser colocado em prática para que o titular tenha real acesso a informações tais como: quais dados pessoais são coletados, como são tratados, e para quais finalidades, dentre outras.

A questão da implantação da transparência na proteção de dados está em *como* compreender sua natureza. Enquanto tratada apenas como princípio a ser aplicado na relação com o usuário, a transparência será praticada sob uma perspectiva puramente formal, como requisito legal a ser cumprido. No entanto, não há cisão entre a questão de fato e a questão de direito relacionadas à transparência. Melhor dizendo, a transparência não está desgarrada dos fatos a que ela visa proteger. Os fatos e o direito se entrelaçam na transparência; ou seja, os fatos relacionados ao usuário consumidor de produtos e serviços de tecnologia dão suporte às normas jurídicas que disciplinam a transparência nessa relação. Esse vínculo entre ambos mostra o

equívoco de tratar transparência como mera formalidade, prevista de antemão pela lei, a ser cumprida pela organização.

Voltamos ao elemento dinâmico da inovação. Essa dinamicidade exige um tratamento igualmente dinâmico para a transparência, de modo que ela seja colocada em prática em situação que vá além do formalismo estático. Raíssa Moura Ferreira e Daniela Motta Monte Serrat Cabella (2020) discorrem que essa é uma maneira de a organização alcançar o público de modo mais significativo, conectando-se com o modo de pensar do público-alvo, sob comunicação em linguagem simples e acessível que considere o modelo mental do público-alvo. Dessa forma, o usuário consumidor de produtos e serviços de *IoT* de fato passa a entender a informação que está sendo transmitida e, ao mesmo tempo, não se sente incomodado com a disponibilização de seus dados pessoais ao fazer uso do serviço ou dispositivo de *IoT*. Essa é uma maneira de tornar as relações mais transparentes *de fato* ao se levar em consideração a experiência do usuário em sua jornada de contato com o serviço ou produto.

4. TRANSPARÊNCIA DE DIREITO E TRANSPARÊNCIA DE FATO

Estabelecemos o conceito de *transparência de direito* como aquela que está direcionada à interpretação e aplicação formal da lei. Esse conceito pode ser exemplificado com o que está exposto no artigo 6º, inciso VI da LGPD (Brasil, 2018), ao determinar que as informações sobre o tratamento de dados pessoais devem ser *facilmente acessíveis*. Isso significa, por exemplo, que essas informações devem ser colocadas de forma relativamente ostensiva nos aplicativos de *smart speakers*, nas opções da *smart tv*, e no *smart watch*. Essa previsão legal pode ser interpretada, portanto, como uma obrigação de que essas informações sejam colocadas em um local fácil de ser encontrado, sem muitas camadas de comandos e etapas no fluxo de interação com o produto de *IoT* até a sua disponibilização.

A transparência de direito pode ainda ser compreendida como a implementação prática dos tópicos mencionados no artigo 9º da LGPD (Brasil, 2018), tais como: acesso facilitado a informações como finalidade específica do tratamento; forma e duração do tratamento; identificação do controlador; informações de contato do controlador; informações sobre o uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes; e direitos do titular.

A *transparência de fato*, por sua vez, realiza o cumprimento material da lei, sendo direcionada à experiência[5] do usuário em toda a jornada de decisão, contratação e pós-venda, e à dinâmica da gestão de riscos à privacidade[6]. Também tem base legal, mas necessita da aplicação de elementos extrajurídicos para sua realização integral. No caso dos *smart watch*, podemos dizer que, além do acesso facilitado às informações – que devem ser disponibilizadas de forma ostensiva –, também (i) devem ser incluídos ícones que possam apoiar a transmissão da informação (os quais demandam a aplicação de conhecimentos de *User Interface – UI* para seu desenho e escolha do local mais adequado para sua disponibilização na interface), (ii) deve-se apresentar cada informação de privacidade no contexto mais pertinente da jornada do usuário no uso desse dispositivo de *IoT*, como os pedidos de permissão de coleta de dados de localização e batimento cardíaco no momento em que as funcionalidades que delas dependem forem ativadas pelo usuário, de modo a evitar a "fadiga do consentimento", e (iii) havendo qualquer mudança no contexto operacional ou do produto que gere um novo risco ao tratamento dos dados sensíveis coletados por meio desse dispositivo, o usuário deve ser informado em tempo hábil e por múltiplos canais de comunicação envolvidos em sua jornada de experiência com o produto – como e-mail, mensagem em aplicativo de comunicação instantânea e notificação via sistema do próprio dispositivo – para tomar uma decisão informada e consciente em relação à continuação ou não do uso do dispositivo, por exemplo.

Assim, verifica-se que a transparência de fato acompanha a dinamicidade das relações entre o usuário consumidor de produtos e serviços de tecnologia e a organização que os fornece. Em última análise, muito além da certeza de que há boa-fé em relação ao tratamento de dados, a transparência de fato gera e fortalece, no titular de dados, um vínculo de confiança com a organização por meio da aplicação dos

5. A Experiência do Usuário (*User Experience – UX*) "inclui todos os aspectos da interação entre o usuário final com a empresa, seus serviços e seus produtos", até mesmo os aspectos de *layout* e *design* da interface (*User Interface – UI*). (fonte: Norman, D; Nielsen, J. (2023). The Definition of User Experience (UX). Nielsen Norman Group. Acesso em 26 de março de 2023. Retirado de https://www.nngroup.com/articles/definition-user-experience/)
6. Em outras palavras, não sendo meramente um reflexo estático da análise realizada no momento de lançamento do serviço, produto ou funcionalidade, mas acompanhando sua evolução e atualização e seus reflexos em todas as etapas da gestão de risco.

elementos não jurídicos. Por outro lado, a ausência ou insuficiência da transparência de fato faz com que emerjam situações antiéticas, dando ocasião a riscos como o de (i) quebra de confiança na relação usuário-organização, (ii) danos à privacidade que poderiam ser evitados caso o usuário tivesse clareza e ciência integral em relação ao tratamento de seus dados pessoais e tivesse, em consequência, a oportunidade de configurar seus dispositivos de *IoT* de forma mais protetiva à sua privacidade; (iii) investigação por entidades públicas; (iv) multas administrativas; (v) ações judiciais; (vi) rescisões contratuais e perda de oportunidades de negócio; (vii) impactos operacionais na alocação de pessoas de diversos times e departamentos para atividades relacionadas a resposta a incidentes com dados pessoais, resposta a autoridades públicas, bem como a questionamentos de clientes e da mídia; (viii) rombo financeiro que, a depender da situação, pode ser irrecuperável e levar à demissão de executivos e funcionários.

Pode-se afirmar, em resumo, que a ausência de transparência de fato é insustentável, pois a inovação tecnológica e até mesmo a organização que a desenvolveu não se sustentam a longo prazo se tiverem que lidar constantemente com os fatores citados.

5. A TRANSPARÊNCIA DE FATO EM RELEVO NA ISO 31700

A transparência se realiza de fato quando as informações sobre o tratamento de dados efetivamente atendem aos requisitos legais aplicando os requisitos de comunicação ao consumidor determinados pelo tópico 5 da ISO 31700-1 (2023) de *Privacy by Design* (Cavoukian, 2011), informando, por exemplo, as mudanças nos riscos à privacidade de modo a capacitar o usuário a a gerenciar esses riscos de forma eficaz (tópico 5.2, "Fornecimento de informações de privacidade") – requisito esse intimamente ligado ao monitoramento e atualização da avaliação de risco (aspecto dinâmico), referenciado pelo item 6.5 da mesma ISO (Brasil, 2023). Uma gestão de riscos eficaz é, portanto, essencial para o cumprimento da transparência de fato.

Além disso, o tópico 5.5 (Brasil, 2023) aborda a comunicação de privacidade para uma população de consumidores diversificada. Segundo ele, é necessário utilizar canais variados para a transmissão dessa informação, tornando possível o esclarecimento de dúvidas, comentários e resolução de reclamações de modo a garantir uma

experiência de consumo aceitável. A melhor maneira de se colocar esse requisito em prática é alinhar a comunicação de privacidade com a jornada do usuário em toda a sua extensão de contato com o produto ou serviço (de *IoT*, por exemplo), desde o momento de pré-experiência até a pós-experiência. Utilizar o Mapa da Jornada do Usuário com *Privacy by Design* da *Complete Privacy* (Cabella e Fereira, 2023) é uma medida de *Privacy by Design* (Cavoukian, 2011) que atende ao princípio de Privacidade Incorporada ao *Design*, e pode e deve ser revisto e atualizado em consonância com a dinamicidade da gestão de riscos à privacidade do produto ou serviço a que se refere, e ainda dá suporte para evidenciar quais os momentos na jornada do usuário e canais mais adequados de acordo com sua experiência para realizar a transparência de fato em relação aos aspectos que tocam a privacidade.

Esses são exemplos de uma abordagem do princípio da transparência no *framework* de *Privacy by Design*[7](Cavoukian, 2011), fazendo-o ir *para além da lei*, concretizando (transparência de fato em contraposição à transparência de direito) na prática, e não somente formalmente, o exercíco da transparência.

Outro elemento que proporciona efetividade material à transparência é o conceito de Ética Sustentável (Cabella e Monte-Serrat, 2022), que garante a extensão da transparência no tempo e sincroniza-a com a inovação, proporcionando sustentabilidade. Passemos, agora, à análise desse conceito.

6. ÉTICA SUSTENTÁVEL, INOVAÇÃO E TRANSPARÊNCIA (DE FATO)

O entendimento *relacional* da transparência de fato[8] torna claro que situações práticas comprovam que leis e regulamentos não são suficientes para compreender a inovação, cujo processo é dinâmico e se estende no tempo. Isso pode ser observado na pesquisa de Felzmann et al. (2019), em que discorrem sobre o fato de auditorias de algoritmos apontarem para vieses problemáticos. Os autores mencionam que a tentativa de transparência (de direito) ao oferecer ao usuário tecnologia de código aberto, que dão acesso aos modelos de aprendizado de máquina, não trouxe a solução adequada para a proteção de dados. Outra sugestão dos autores é a possibilidade de

7. Maiores informações sobre o *framework* são encontradas no item 6.2 deste Capítulo.
8. Vide Seção 4, sobre transparência de direito e transparência de fato.

que colaborações multidisciplinares entre engenheiros, cientistas sociais, advogados, filósofos e eticistas auxiliem na implementação da transparência no próprio *design* da tecnologia.

Contornar a complexidade da implementação de fato do princípio da transparência é um grande desafio. Zuboff (2019) menciona a situação paradoxal em que uma organização usa de transparência no processo de vendas e o usuário, em seu envolvimento, não se dá conta de que essa transparência é falha. Felzmann et al. (2019) alertam para o fato de que a transparência deve ser significativa e confiável aos olhos dos usuários, e ter utilidade e limitações aos olhos dos formuladores de políticas. Normas europeias, por sua vez, estabelecem que a transparência deve chegar efetivamente ao titular dos dados por meio de situações como: a de que o controlador seja aberto e claro ao tratar com o titular dos dados; de que as informações sejam transmitidas de maneira clara e concisa, de maneira acessível ao titular dos dados, de forma apropriada e inteligível, por meio de diferentes canais e suportes (EDPB, 2019). No entanto, essas medidas não têm levado, a contento, a resultados de transparência eficazes em relação à privacidade dos usuários de produtos e serviços de tecnologia, como a *IoT*.

Em nosso *e-book* sobre a "Ética Sustentável nas Decisões em Tratamento de Dados no Contexto da Inovação" (Cabella e Monte-Serrat, 2022) observamos que computação, engenharia, bioinformática, *IoT* têm impactos no comportamento humano no tempo presente e no tempo futuro, o que dificulta a tutela da proteção de dados (nela, considerada a prática da transparência) do usuário de tecnologias inovadoras. Para contornar os desafios impostos pela dinâmica da inovação, desenvolvemos o conceito de Ética Sustentável, que é tratado em mais detalhes a seguir.

6.1. ÉTICA SUSTENTÁVEL NO TRATAMENTO DE DADOS PESSOAIS

Enquanto a tecnologia continuar sendo tratada como *execução de algoritmos usando dados de alguém*, tudo o que a envolve, inclusive os princípios éticos e de transparência, é tratado como algo estático. Em nosso *e-book* (Cabella e Monte-Serrat, 2022), mostramos a tecnologia sob a perspectiva de um processo dinâmico, que deve ter um acompanhamento igualmente dinâmico dos princípios éticos e de transparência que a regulam. Afirmamos, ainda, que esse é o caminho para garantir

sustentabilidade na segurança de dados e na inovação.

O livro (Cabella e Monte-Serrat, 2022) sincroniza os impactos desta última na aplicação dos princípios éticos, abarcando a permeabilidade da Internet das Coisas, *IoT*, no cotidiano dos indivíduos. Na ética sustentável, o tratamento de dados se dá de acordo com valores impostos por normas, regras e princípios sem perder de vista os efeitos presentes e futuros que a inovação provoca.

Discutimos (Cabella e Monte-Serrat, 2022), ainda, a questão de que, embora ética e proteção de dados devam estar unidas na prevenção de danos à privacidade do usuário, surgem, na prática, situações de tratamento de dados ilegal, ou legal porém antiético. Por esse motivo, descrevemos a ética sustentável como algo que vai além da aplicação de regras e normas, a fim de atingir a equidade, ou seja, o respeito, o senso de justiça em relação aos titulares dos dados.

Também propusemos (Cabella e Monte-Serrat, 2022) que os conceitos de ética de convicção e responsabilidade (Weber, 1998; Corrêa, 2016) sejam combinados para equilibrar a aplicação de leis, princípios e práticas éticas no complexo cenário de decisões e operações de tratamento de dados pessoais. Essa combinação gera um equilíbrio que estimula um ciclo autoalimentado e recarregável por meio das práticas internas da organização, garantindo, assim que práticas sustentáveis abarquem toda a complexidade de questões éticas no tratamento de dados pessoais.

É fato que o uso insustentável de dados pessoais aumenta as chances de manipulação para suprimir direitos e liberdades ou cometer crimes. A aplicação de uma ética sustentável previne danos e garante desenvolvimento tecnológico. Para que isso ocorra no contexto da inovação, é preciso sincronizar elementos e ações, como, por exemplo, a análise ética *by design*, realizada quando o produto, serviço ou funcionalidade é projetado e durante cada etapa de revisão e atualização do produto, proporcionando alinhamento integral entre a tecnologia e a ética. Também é fundamental haver coalizão, respeito mútuo e compromisso entre todas as partes envolvidas em um mesmo contexto (Cabella e Monte-Serrat, 2022), uma vez que são interdependentes.

Em nosso entendimento (Cabella e Monte-Serrat, 2022), a aplicação de princípios éticos, torna-se sustentável quando a análise, interpretação e decisão em relação a todos os aspectos do tratamento de dados (inclusive a prática da transparência) são

consideradas em sintonia com os valores impostos por normas, regras e princípios éticos previamente estabelecidos, sem perder de vista os efeitos presentes e futuros e o contexto dinâmico da inovação. E esse contexto dinâmico está, por sua vez, também atrelado à transparência de fato[9] e à gestão eficaz de riscos à privacidade, garantindo, a um só tempo, o acesso à informação de maneira agradável e que faça sentido ao usuário consumidor de produtos e serviços de tecnologia, e reduzindo riscos que poderiam ser maiores tanto no presente como no futuro devido à falta de transparência material.

Uma abordagem instrumental do tipo *checklist* de recomendações, quanto ao quê fazer ou não fazer eticamente falando, não é favorável ao ambiente tecnológico justamente por não acompanhar a dinâmica da inovação. Também não é favorável a mera aplicação da transparência de direito, que apenas cumpre preceitos legais. A solução para desafios na inovação de *IoT* está na flexibilidade proporcionada pela ética sustentável, que é proativa, dinâmica e capaz de automonitorar o ambiente de inovação tecnológica, proporcionando consistência, transparência de fato e sustentabilidade ao tratamento de dados, ao produto ou serviço que dele depende e à organização que o disponibiliza (Cabella e Monte-Serrat, 2022).

6.2 O *FRAMEWORK* DE *PRIVACY BY DESIGN* E A ISO/IEC 31700

Os limites e possibilidades de interferência da tecnologia na vida pessoal e nos direitos fundamentais dos indivíduos estão previstos em parecer do *European Data Protection Supervisor*, (EDPS 2018). Esse estudo revela de que o uso inapropriado de dados pessoais foi intensificado e, nesse contexto, a modelagem e o uso da tecnologia devem respeitar os direitos dos indivíduos, embora as inovações tecnológicas sejam movidas por interesses econômicos.

A determinação da *proteção de dados por design e por padrão*, prevista no artigo 25 do *General Data Protection Regulation* (GDPR, 2016), tem origem no conceito de *Privacy by Design*, desenvolvido pela Dr. Ann Cavoukian, PhD (2011), ex-Comissária de Informação e Privacidade de Ontário, Canadá. O objetivo do *framework* criado por ela é viabilizar a gestão responsável da informação no contexto da inovação

9. Vide Seção 4.

acelerada, da competição em escala global e da complexidade crescente dos sistemas, que traz consigo grandes desafios para a privacidade.

Cavoukian (2011) defende que o futuro da privacidade não pode estar restrito às estruturas regulatórias, mas deve tornar-se um padrão para modo de as organizações operarem, a fim de que se garanta a privacidade de um lado e vantagens competitivas sustentáveis às organizações de outro. Para isso, Cavoukian (2011) estabeleceu sete princípios fundamentais, quais sejam:

> i. *Proativo e não reativo; Preventivo e não corretivo* (antecipação de ameaças, prevenção e redução de riscos à privacidade antes que se concretizem);
>
> ii. *Privacidade por Padrão* (proteção máxima à privacidade de forma automática, sem a necessidade de configuração por parte do usuário);
>
> iii. *Privacidade Incorporada ao Design* (privacidade considerada desde o início da criação e desenho de uma solução e incorporada desde então aos processos organizacionais e procedimentos operacionais);
>
> iv. *Funcionalidade Total – Soma-Positiva, não soma zero* (acomodação de todos os interesses e objetivos em uma abordagem ganha-ganha (privacidade + segurança + interesse do negócio + experiência do usuário + conformidade jurídica + ética + transparência + gestão de risco + viabilidade técnica etc.);
>
> v. *Segurança de ponta a ponta – Proteção Completa do Ciclo de* Vida (garantia da implementação de medidas técnicas e administrativas de Segurança da Informação ao longo de todo o ciclo de vida dos dados pessoais, de modo a protegê-los de todos os tipos de tratamento não autorizado);
>
> vi. *Visibilidade e Transparência – Mantenha Aberto* (fornecimento de informações claras e transparentes para viabilizar a verificação se de fato o tratamento ocorre como informado ao usuário), e
>
> vii. *Respeito pela Privacidade do Usuário – Mantenha Centrado no Usuário* (colocar o usuário no centro de todas as decisões relacionadas ao tratamento de seus dados pessoais).

O *framework* (Cavoukian, 2011) busca, ao final, aprimorar a privacidade no uso de tecnologias, adotando uma dimensão ética consistente com os princípios e valores traçados pelos direitos fundamentais. Esse direcionamento está em linha com as diretrizes sobre a implementação de proteção de dados *by design* e *by default* do EDPB

(2019), segundo as quais a equidade baseada na ética (que deve antever o impacto mais amplo do processamento de dados sobre os direitos e a dignidade dos titulares, conforme o tópico 3.3, p.18) deve dar suporte ao direito do titular de acesso à informação (transparência).

A norma ISO 31700-1 (2023) também destaca o papel fundamental da transparência para não apenas colocar em prática direitos fundamentais, mas também empoderar o consumidor e conquistar sua confiança (Introdução, p.vii).

ISO 31700 (2023) é um documento publicado pela Organização Internacional de Normalização para fornecer requisitos e recomendações de alto nível para organizações que protejam a privacidade do consumidor desde o *design*.

A privacidade por *design* liga-se ao comportamento e jornada de experiência do consumidor em sua relação com o produto (o que também pode ser estendido e aplicado a um serviço). Por esse motivo, a institucionalização do processo de privacidade deve estar presente desde o início nos ecossistemas de informações, compreendendo as tecnologias e as organizações que nele operam (ISO 31700-1, p.vii) (ISO, 2023). Desse modo, a privacidade e a proteção do consumidor são consideradas de maneira integrada. A deficiência de informação nesse ecossistema pode aumentar a vulnerabilidade do consumidor, gerando um risco à sua privacidade.

A comunicação com o consumidor está entre os requisitos da ISO 31700 (2023), em razão de seu impacto na privacidade. Explicações e compromissos expostos com clareza e de modo acessível e verificável são esperados no gerenciamento da privacidade. Assim, espera-se que o consumidor tenha sua tomada de decisão facilitada ou que incidentes ou erros pronta, clara e satisfatoriamente sejam explicados. Essa transparência na comunicação com o consumidor dá apoio à responsabilidade para que o usuário tome as medidas cabíveis em tempo hábil, e pode ocorrer por meio de documentos (manual, avisos ou instruções de privacidade), publicidade, mensagem direta, dentre outras formas. As oportunidades de a organização manifestar, ao consumidor, informações transparentes estão em todos os elementos do ciclo de vida do produto, e isso se aplica também ao contexto da *IoT*.

De todo o exposto nesta Seção, depreendemos que a comunicação com o usuário consumidor no contexto da *IoT* está sujeita a dois tipos de transparência:

i. A *transparência de direito*, direcionada à interpretação e aplicação da lei. Exemplo

disso no cenário da *IoT* está no artigo 6º, inciso VI da LGPD (Brasil, 2018), que determina que as informações sobre o tratamento de dados pessoais devem ser *facilmente acessíveis*. Isso significa que essas informações devem ser *disponibilizadas* de forma relativamente ostensiva nos aplicativos de *smart speakers*, nas opções da *smart tv*, e no *smart watch*. Ou seja, essas informações devem ser colocadas em um local fácil de ser encontrado *e acessado (alcançado, aberto e explorado)*, sem muitas camadas de comandos e etapas no fluxo de interação com o produto de *IoT* até a sua disponibilização.

ii. A *transparência de fato*, por sua vez, é direcionada à *jornada e experiência* do usuário, *acompanhando* a *dinâmica* da gestão de riscos à privacidade. No âmbito da *IoT*, por exemplo, temos o caso dos *smart locks* citado na ISO/TR 31700-2 (ISO, 2023), em que um consumidor interessado em adquirir o produto (fase de pré-experiência na jornada do usuário) *interage* com o serviço de atendimento ao cliente, ou seja, a *transparência de fato é relacional e não apenas formal*. Considerando-se a orientação dos tópicos 5.5.3 *d* e *e* da ISO 31700-1 (ISO, 2023), que determina o uso de meios diversificados para a comunicação com os consumidores, conclui-se que esse é um dos meios de fornecimento de informações a respeito do tratamento de dados pessoais que (i) faz sentido para o momento de pré-experiência do usuário em relação ao produto, (ii) tem ligação com a situação vivenciada pelo consumidor e respeita seus sentimentos naquele momento, e (iii) reflete o cenário atual de risco à privacidade do titular em relação ao uso do dispositivo de *IoT* (que pode já não ser o mesmo da época em que a primeira análise de risco *by Design* foi realizada na etapa de criação do produto). Em última análise, pode-se dizer que a transparência de fato dá ao titular de dados a certeza de que há boa-fé em relação ao tratamento de seus dados.

7. TRIPÉ DA ACELERAÇÃO DA INOVAÇÃO: ABORDAGEM INTEGRADA SOBRE A TRANSPARÊNCIA

A inovação em *IoT* implica velocidade para se manter relevante. Nesse cenário, exigências de conformidade jurídica, implementação de melhores práticas e reflexões sobre o processo de desenvolvimento ou melhoria de produtos ou serviços costuma ser interpretadas como entraves que podem atrasar o lançamento no mercado. No entanto, a vivência no setor de tecnologia revela que a combinação do *framework* de *Privacy by Design* (Cavoukian, 2011), hoje consolidado pela ISO 31700 (ISO, 2023), com a implementação de melhores práticas para a *gestão de riscos* e com

a *reflexão dinâmica* sobre princípios éticos (ética sustentável) podem, todos atrelados, funcionar como um *Tripé de Aceleração da Inovação* (Cabella, 2022), garantindo, assim, inovação responsável e sustentável. Esse Tripé sustenta e promove todos os demais princípios legais, como o da transparência (de fato).

Por que Tripé? Porque, assim como são necessários no mínimo três pontos de apoio para sustentar um banco de madeira sobre um plano, a organização, igualmente, precisa da implementação desse conjunto mínimo para sustentar a si mesma e o desenvolvimento da inovação na Era da Economia Digital. Se apenas um ou dois pilares estiverem implementados, ainda haverá instabilidade, assim como um banco de madeira de apenas um ou dois pés. O *framework* de *Privacy by Design* (Cavoukian, 2011), a ética sustentável e gestão de riscos, cada um deles constitui um dos pés do Tripé. Eles sustentam, em sua complexidade *relacional* e dinâmica a organização, de modo que esta última consiga vislumbrar possibilidades e alcançar patamares de inovação que antes não conseguia (da mesma forma que uma pessoa enxerga e alcança coisas que antes de subir em um banco não conseguia).

E por que *aceleração*? Antigamente, os carros não tinham cinto de segurança. Por esse motivo, esses veículos precisavam andar muito devagar – se acelerassem e depois bruscamente precisassem frear ou fazer uma conversão, as pessoas dentro dele poderiam se machucar e até perder a vida. Somente com o advento do cinto de segurança – com destaque para o mais seguro atualmente que é o de três pontos – é que foi possível proporcionar a aceleração, o ganho de velocidade. O Tripé também vai trazer segurança (jurídica, ética e na gestão de riscos) para que a organização acelere, ganhe velocidade no processo de inovação, evitando, nesse processo, danos aos titulares de dados pessoais e a si própria.

A experiência revela que a aplicação do suporte do Tripé à transparência (de fato) contribui de forma positiva para a reputação da organização, para a consistência de sua atuação, e confiança do mercado, da sociedade e das autoridades quanto aos produtos e serviços ofertados. Isso também contribui para a atração de maiores quantidades de investimento (especialmente quando há *due dilligence* de Privacidade e Proteção de Dados) e recursos, os quais, por sua vez, fomentam a inovação. O *Tripé de Aceleração da Inovação* (Cabella, 2022) contribui, ainda, para o sucesso da inovação, com a prevenção de danos à privacidade dos titulares de dados pessoais, sustentando as organizações a longo prazo, proporcionando velocidade na criação de melhorias e

novos produtos (evitando a correção, o retrabalho), e prevenindo ou evitando os percalços da falta de ética e transparência (de fato).

Lembramos, ainda, que esses três pilares são de responsabilidade de toda e qualquer organização, de todos os departamentos e times, e não só de *Compliance*, Jurídico, ou de Governança. Até mesmo os desenvolvedores, por exemplo, precisam conhecer os dilemas e implicações éticas a longo prazo daquilo que está sendo projetado ou em processo de desenvolvimento. Isso os capacita a identificar e apontar potenciais riscos e, consequentemente, a colaborar na correta gestão desses riscos. O conhecimento dos princípios do *framework* de *Privacy by Design* (Cavoukian, 2011), mais especificamente, os habilita a propor e implementar formas de lançar um produto já aderente a todas essas melhores práticas, evitando danos, retrabalho e perda de tempo e recursos.

São os três, portanto, os propulsores do foguete da inovação: *framework* de *Privacy by Design*, implementação de melhores práticas para a *gestão de riscos*, e a reflexão dinâmica sobre princípios éticos (*ética sustentável*) (Cabella, 2022). Não é suficiente o lançamento de um produto sem que esses três componentes estejam presentes, pois, do contrário, essa inovação não irá se sustentar. A falta desse conjunto pode levar à concretização de altos riscos, danos aos titulares de dados, danos à reputação da empresa.

Diversas pesquisas revelam que condutas antiéticas, a falta de uma gestão efetiva de risco, a falta da implementação de medidas de *Privacy by Design* (Cavoukian, 2011), como as do princípio de segurança de ponta a ponta, impactam negativamente o próprio negócio e a inovação.

Um trabalho de conscientização da alta liderança das organizações torna-se necessário para que essa visão estratégica de investir na implementação efetiva do Tripé seja adotada. E, quando adotada, torna-se um diferencial competitivo no mercado, algo que agrega valor ao produto.

A implementação do Tripé de Aceleração da Inovação (Cabella, 2022) e a visibilidade disso (comunicação) para a sociedade, para o mercado e para as autoridades públicas faz toda a diferença. A transparência em relação às melhores práticas implementadas para apoiar a proteção da privacidade reforça o vínculo de confiança do consumidor em relação à organização responsável pelo produto de *IoT* que ele utiliza

em seu dia a dia, por exemplo.

Por outro lado, quando há qualquer tipo de inconsistência, de falácia, engodo, falta de transparência de fato ou há um risco que não é endereçado da forma correta, ou decisões antiéticas são tomadas quanto ao tratamento de dados pessoais no contexto da inovação, a harmonia não se instala. Nesse contexto, não há consistência entre os fatores envolvidos, nem na comunicação entre as partes interessadas. Não há, portanto, sustentabilidade. Esta se instala somente quando, desde a concepção de um projeto, produto, serviço, até a sua entrega, e em todas as relações criadas, há transmissão de ideias, convencimento, comunicação de maneira a garantirem sucesso no presente e extensivo para o futuro.

O *modo relacional* de administrar o *framework* de *Privacy by Design*, a gestão de riscos e a implementação de princípios éticos é que mantém coeso e funcional o Tripé de Aceleração da Inovação (Cabella, 2022), que propulsiona a transparência de fato no contexto da inovação. Esses três pilares se relacionam através de muita *comunicação*, e a comunicação só é possível por meio da *linguagem*. A linguagem é a *cola* que *relaciona* todos os componentes unindo-os no Tripé de Aceleração da Inovação. Qualquer atitude antiética, ou que de alguma forma impacte negativamente qualquer um dos pilares, será comunicada na forma de um *ruído* na comunicação.

A não implementação do Tripé gera inconsistência, e, em consequência, instala a insustentabilidade. Isso afeta as partes envolvidas e qualquer projeto de sustentabilidade, seja da inovação, seja da própria organização.

CONCLUSÃO

Neste Capítulo, vimos que a *IoT* não deve ser apreendida como algo descentrado e abstrato, mas como algo que produz impactos na subjetividade do usuário, daí a necessidade de proteção dos dados dele. A relação usuário-*IoT* é complexa e vai além das regulamentações legais, pondo em xeque princípios éticos e de transparência. A privacidade por *design* foi incorporada pelas regulamentações porque considera tecnologias, organizações e usuários de maneira integrada, de modo que qualquer deficiência de informação acarreta risco à privacidade do consumidor vulnerável.

Defendemos que a regulamentação da comunicação com usuários de *IoT* necessita, em razão da contínua inovação, assegurar sustentabilidade que produza reflexos

positivos para o futuro, evitando descompasso entre a realidade vivenciada pelo consumidor e os estatutos disciplinadores dessa realidade.

De modo mais restrito, este Capítulo traz exemplos práticos de implementação da transparência de fato na comunicação com os consumidores, segundo requisitos da ISO 31700. A publicação da ISO 31700 (2023) foi oportuna, pois trouxe controles objetivos e específicos que incidem na concepção do produto, na sua funcionalidade, operação e manutenção, proporcionando apoio às organizações na comunicação com os usuários de seus produtos, especialmente as comunicações de privacidade no campo da *IoT* (ISO 31700-2) (2023).

De modo mais amplo, este Capítulo propõe uma sincronia entre a inovação e as práticas éticas e transparentes efetivas através da adoção do Tripé de Aceleração da Inovação (Cabella, 2022). Esse Tripé proporciona inovação responsável na atualidade e no futuro, com a aplicação do conceito de Ética Sustentável (Cabella e Monte-Serrat, 2022), uma vez que esta implica mudanças de contexto durante a operação da *IoT* ou durante a gestão de riscos à privacidade. A questão do desenvolvimento da inovação responsável não está no desenho ou redesenho do produto em si, mas está em *como* aplicar leis e princípios na comunicação com os usuários dos dispositivos tecnológicos e serviços inovadores, como no contexto da *IoT*. A comunicação formal provoca estagnação da transparência e da ética, que não acompanham a inovação. A comunicação com usuários de *IoT* por meio do *Privacy by Design* (ISO 31700-1) (2023) é uma das formas possíveis de colocar em prática a ética sustentável. A comunicação embasada no Tripé de Aceleração da Inovação adota uma perspectiva mais ampla e relacional, que vai além do formalismo estático das regulamentações, atrelando transparência de direito, transparência (dinâmica) de fato, a dinâmica da gestão de riscos à privacidade e a dinâmica da ética sustentável.

Enquanto a legislação e as decisões judiciais permanecem sempre um passo atrás da inovação, o Tripé de Aceleração da Inovação abarca a visão de futuro, da ética que vai sustentar essa inovação e garantir a transparência de fato no contexto da *IoT*.

REFERÊNCIAS

Brasil, (1990). Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor, CDC). Acesso em 26 de março de 2023.

Retirado de https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

Brasil (2014). Lei nº 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). Acesso em 26 de março de 2023. Retirado de http://www.planalto.gov.br/CCivil_03/_Ato2011-2014/2014/Lei/L12965.htm

BRASIL (2018). LGPD- Lei Geral de Proteção de Dados. Lei n. 13.709, de 14 de Agosto de 2018. Redação dada pela Lei 13.853 de 2019. Acesso em 02 de março de 2023. Retirado de https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Cabella, D. M. (2022). *Tripé de Aceleração da Inovação*: conceito e prática para as organizações. Grupo de Estudo Direito e Tecnologia Tech Law, IEA-USP, C4AI-USP-IBM-FAPESP. Acesso em 26 de março de 2023. Retirado de https://www.youtube.com/watch?v=b1HemhIX0Uc

Cabella, D. M.; Monte-Serrat, D. (2022). *Ética sustentável nas decisões em tratamento de dados no contexto da inovação* 1. ed., Rio de Janeiro. ISBN 978-65-00-45707-0. Acesso em 22 de março de 2023. Retirado de https://iapp.org/media/pdf/resource_center/sustainable-ethics-cabella-monte-serrat-portugese-edition.pdf

Cabella, D.; Ferreira, R. (2023). Mapa da Jornada do Usuário com *Privacy by Design* da *Complete Privacy*. Acesso em 22 de março de 2023. Retirado de https://miro.com/miroverse/user-journey/

Cavoukian, A. (2011). *Privacy by Design. The 7 Foundational Principles* - Implementation and Mapping of Fair Information Practices. Acesso em 22 de março de 2023. Retirado de https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf

Code of Fair Information Practice, CFIP (1973). Summary and Recommendations. Adotado pelo Advisory Committee on Automated Personal Data Systems. Acesso em 26 de março de 2023. Retirado de https://archive.epic.org/privacy/hew1973report/Summary.htm

Corrêa, R. D. S. S. (2016). O limite entre a ética da convicção e a ética da responsabilidade no desempenho policial militar nos centros urbanos. *Perspectivas*: Revista de Ciências Sociais, 47. Disponível em: https:// periodicos.fclar.unesp.br/perspectivas/article/view/5795/7001.

EDPB, European Data Protection Board on Data Protection by Design and by Default (2019). Acesso em 22 de março de 2023. Retirado de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

EDPS, European Data Protection Supervisor (2018). Opinion 5/2018. Preliminary Opinion on privacy by design. Acesso em 6 de Março de 2023. Retirado de https://edps.europa.eu/sites/edp/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf

Fair Information Practice Principles, FIPPs (2023). United States government. Acesso em 26 de março de 2023. Retirado de https://www.fpc.gov/resources/fipps/

Felzmann, H.; Villaronga, E. F.; Lutz, C.; Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, *6*(1), 2053951719860542.

Ferreira, R; Cabella, D. (2020). Escrevendo e implantando os avisos de privacidade (*privacy notices*) na coleta do consentimento válido. In *Data Protection Officer* (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. Opice Blum, R; Vainzorf, R.; Moraes, H. F. (Orgs.) 1.ed. São Paulo: Thomson Reuters Brasil.

GDPR, União Europeia - General Data Protection Regulation. Regulation (EU) 2016/679 regarding Automated Processing of Personal Data. Acesso em 02 Maio, 2023. Retirado de https://gdpr-info.eu/

Haase, Jan; Alahmad, Mahmoud; Nishi, Hiroaki; Ploennigs, Joern; Tsang, Kim Fung (2016). The IOT mediated built environment: A brief survey. *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*. pp. 1065–1068. doi:10.1109/INDIN.2016.7819322. ISBN 978-1-5090-2870-2. S2CID 5554635.

ISO, International Organization for Standardization, 31700-1 (2023). Consumer protection — Privacy by design for consumer goods and services. Retirado de https://www.iso.org/obp/ui/#iso:std:iso:31700:-1:ed-1:v1:en

Monte-Serrat, D. (2021). Operating language value structures in the intelligent systems. *Advanced Mathematical Models & Applications*, *6*(1), 31-44.

Monte-Serrat, D; Cabella, DMS, (2022). Ética sustentável no Metaverso: uma proposta para a proteção da privacidade. In Palhares, F. (Org.) *O Direito no Metaverso*. Ed Thomson Reuters Brasil – RT, pp 113-130 ISBN 978-65-260-0609-2

Monte-Serrat, D. ; Cattani, C. (2022). Applicability of emotion to intelligent systems. *Information Sciences Letters; Natural Sciences Publishing: New York, NY, USA*, *11*, 1121-1129.

Paal, P.; Pauly, D (2018) *Kommentar zur Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz*. Munich: C.H. Beck.

Thielova, L. (2023). One Trust Blog. Regulations / *7 steps to comply with ISO 31700-1:2023* (standard on Privacy by Design). February 10, 2023.Acesso em 06 de Março de 2023. Retirado de https://www.onetrust.com/blog/7-steps-to-comply-with-iso-31700-12023-standard-on-privacy-by-design/

União Europeia, U. E. (1995). Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial nº L 281 de 23/11/1995 p. 0031 – 0050. Acesso em 26 de março de 2023. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Weber, M. (1998). *Ciência e política*: duas vocações. São Paulo: Cultrix.

Zuboff, S. (2019). *The age of surveillance capitalism.* The fight for a human future at the new frontier of power: Barack Obama's books of 2019. Profile books.

SMART CITY E A PROTEÇÃO DE DADOS PESSOAIS

Gabriel Ribeiro de Lima

Mestrando em Direito, Tecnologia e Inovação pela Universidade Federal de Minas Gerais. Pós-graduado em Direito de Uso e Proteção dos Dados Pessoais pela PUC Minas. Bacharel em Direito pela Universidade UMA. Bacharel em Administração com ênfase em Comércio Exterior pela Universidade UMA. Advogado.

DOI: https://doi.org/10.59224/dti5.ch10

Resumo: O presente trabalho buscou analisar o SynchroniCity, projeto que estudou a implantação de um mercado único digital de serviços habilitados em IoT nos ambientes urbanos. Verifica-se a arquitetura da rede única de IoT em smart city criada pelo programa. Perquire-se as alternativas encontradas pelo projeto para a adequação da sua arquitetura à lei de proteção de dados pessoais europeia (GDPR).

Palavras-chave: Internet das Coisas; *Smart City*; Proteção de Dados.

Abstract: *The present work sought to analyze SynchroniCity, a project that studied the implementation of a single digital market of IoT-enabled services in urban environments. The architecture of the single network of IoT in smart city created by the program is verified. The alternatives found by the project are investigated for adapting its architecture to the European personal data protection law (GDPR).*

Keywords: *Internet of Things; Smart City; Data Protection..*

1. INTRODUÇÃO

O potencial disruptivo da smart city tem se mostrado ilimitado e vem

transformando o modo de vida das pessoas. Muitas cidades estão investindo em tecnologia digital para melhorar a eficiência de suas atividades, processos e tomada de decisão.

Os exemplos de implantação da tecnologia nas cidades inteligentes variam de mobilidade aprimorada por gerenciamento de tráfego até redução de recursos através de controle inteligente de iluminação pública e coleta de resíduos. A SynchroniCity pretende unificar essas e outras atividades por meio de um mercado digital único comum e padronizado para serviços urbanos habilitados em IoT.

O projeto conta com o apoio da Open & Agile Smart Cities (OASC), organização formada por mais de 100 cidades em todo mundo, que busca o aprimoramento da tecnologia em smart cities. Várias de suas cidades filiadas estabeleceram zonas de referências para a criação do programa piloto de grande escala em IoT.

Esta iniciativa interessa a muitas áreas de estudo, inclusive ao Direito. Do ponto de vista deste trabalho, busca-se entender a funcionalidade da arquitetura do SynchroniCity e identificar as medidas tomadas pelo projeto para a defesa dos dados pessoais bem como para a sua conformidade com o General Data Protection Regulation (GDPR).

Para desenvolver esta questão é fundamental a união de esforços de pessoas de diversas áreas do conhecimento como juristas e cientistas da computação. Portanto, este artigo não tem a pretensão de trazer soluções, até pela ignorância do seu autor. Os seus objetivos são trazer a experiência, as dificuldades e as soluções do velho continente na implantação de dispositivos IoT em smart cities, especialmente quanto a privacidade e a proteção dos dados.

Para isso, foram utilizados materiais sobre Internet of Things e smart city, casos práticos de implantação dessas tecnologias, doutrinas sobre proteção de dados e segurança em IoT, as guidelines sobre o programa SynchroniCity e a legislação específica.

Por fim, o artigo se estruturará em seis partes, incluindo esta introdução. Inicialmente, investigam-se os conceitos de smart city e de dispositivos em IoT, além de detalhar o LSP de nome SynchroniCity (Parte 2). Em seguida, analisam-se as barreiras para a implantação de uma arquitetura em IoT em larga escala e os atributos da rede idealizada pelo SynchroniCity (Parte 3) Após, estuda-se a arquitetura criada

pelo SynchroniCity e seus principais componentes (Parte 4). Posteriormente, verificam-se as medidas adotadas pelo programa para entrar em conformidade com o GDPR, especialmente a adoção de dois encarregados de proteção de dados por cidade (DPO), a confecção de uma Avaliação de Impacto de Proteção de Dados (DPIA) para cidades inteligentes, e a criação de um aplicativo de privacidade (Parte 5). Por fim, faz-se considerações finais (Parte 6).

2. *IOT* EM *SMART CITY:* NOVAS PERSPECTIVAS PARA A PROTEÇÃO DOS DADOS PESSOAIS

Smart City é uma expressão inicialmente criada por grandes provedores de tecnologia da informação e utilizada para o marketing de seus produtos e serviços. Atualmente, não há um consentimento doutrinário sobre o termo e várias organizações governamentais e de pesquisa criaram o seu significado de smart city.

Para Prarahaj e Han[1], *smart city* possui sentidos diferentes que se alteram de acordo com o lugar onde a tecnologia é implantada e o que é implantado. O seu entendimento se relaciona com os recursos disponíveis para a inovação, a prontidão para a mudança e as aspirações e expectativas dos cidadãos.

Por outro lado, Ziosi e outros entendem que s*mart city* pode se referir a adições tecnológicas em antigas cidades para a implementação de novas informações de Tecnologia de Comunicação (TIC) ou sistemas de transporte. Além disso, *smart city* também pode ser utilizado para definir a construção de uma cidade totalmente nova ou o desenvolvimento de um bairro específico[2].

A *International Telecommunication Union* (ITU), agência das nações unidas especializada em tecnologia de informação e comunicação (TIC) define *smart sustainable city* como uma cidade inovadora que usa TICs e outros meios tecnológicos para melhorar a qualidade de vida, a eficiência da operação e dos serviços urbanos e a competitividade, assegurando ao mesmo tempo que atenda às necessidades das

1. ZIOSI, Marta; HEWITT, Benjamin; JUNEJA, Prathm; TADDEO, Mariarosaria; FLORIDI, Luciano, *Smart Cities: Reviewing the Debate about their Ethical Implications* (January 5, 2022). Disponível em SSRN: https://ssrn.com/abstract=4001761 ou http://dx.doi.org/10.2139/ssrn.4001761 (p. 5).
2. Idem, p. 3.

gerações presentes e futuras com respeito aos aspectos econômicos, sociais e ambientais[3].

Assim como a *smart city*, os dispositivos em Internet of Things (IoT) não têm uma definição unanimemente aceita. Iqbal e outros destacam que cada organização elabora o seu conceito de IoT. Além disso, conceituam IoT como um sistema em que os dispositivos estão conectados de tal maneira que eles interagem entre si de forma inteligente uns com os outros e com os seres humanos[4].

Alexandre de Morais, atual ministro do STF, entende IoT como pequenos computadores ou microcomputadores conectados à internet e cloud, destinados a facilitar ou dificultar a vida do ser humano[5]. Estes dispositivos podem ser utilizados tanto para conforto pessoal, como é o caso de residências inteligentes, carros autônomos e relógios inteligentes, quanto para implantações de serviços urbanos, como ocorrem nas smarts cities.

Para Oliveira, IoT está muito além de simplesmente ligar equipamentos por meio de um smartphone. É uma tecnologia capaz de coletar e processar informações do local onde ela se encontra ou da rede da qual o equipamento está conectado[6].

A combinação das tecnologias *smart city* e IoT vem gerando frutos em diversas cidades. Governos de vários países, em parceria com o mercado privado, estão integrando a IoT em diversas atividades urbanas como, na prestação de redes de transportes urbanos inteligentes, instalações atualizadas de abastecimento de água e rede de iluminação pública eficiente, gerenciamento de irrigação, sistema de monitoramento de saúde e aquecimento de edifícios[7].

---

3. INTERNATIONAL TELECOMMUNICATION UNION. *Smart sustainable cites: Na analysis of definitions*. Focus Group Technical Report. 2014. Pg 09 e 10
4. IQBAL, Muhammad Azhar, HUSSAIN, Sajjad, XING, Huanlai, Imran, Muhammad Ali. *Enabling the Internet of Things: Fundamentals, Design, and Apliccations*. Editora John Wiley & Sons Ltda. Primeira edição. 2021. Pg 23
5. MORAES, Alexandre de; HAYASHI, Vitor Takashi. *Segurança em Iot. Entendendo os riscos e ameaças em Internet das Coisas*. Editora Alta Books. 2021 pg13
6. OLIVEIRA, Sérgio de. *INTERNET das COISAS com ESP8266, ARDUINO e RASPBERRY P1*. Editora Novatec LTDA. Junho/2017 primeira edição. Pg 5
7. EUROPEAN COMMISSION *Smarts Cities. Cities using technological solutions to improve the management and efficiency of the urban environment* disponível em: https://ec.europa.eu/info/eu-

Em Barcelona, foram instalados sensores nos postes de energia para ajustar automaticamente a iluminação conforme os níveis de luminosidade, poluição atmosférica e densidade populacional. A cidade ainda oferece sistema que informa os motoristas onde há vagas gratuitas. Já em Singapura, o governo instalou câmeras integradas para monitorar a densidade populacional, a limpeza dos espaços públicos e o movimento dos veículos oficiais[8].

Em Dubai, o governo lançou um aplicativo chamado Dubai Now com mais de 130 serviços inteligentes. Dentre eles estão o pagamento de contas, a renovação de registro de veículo, o acompanhamento de processo de visto e a solicitação de certidões de registro civil[9].

Porém, nem tudo são flores. A natureza heterogênea, distribuída e dinâmica dos dispositivos habilitados em (IoT) criou vários problemas durante a sua aplicação em ambientes públicos, sendo dois deles os riscos a proteção de dados e a privacidade dos cidadãos. Atualmente, vários países pesquisam meios confiáveis para a implantação em grande escala dessa tecnologia no ambiente urbano.

Entre os anos de 2016 e 2019, a Comissão Europeia financiou um Large Scale Pilot (LSP) sobre IoT em cidades inteligentes, organizado pelo programa de investigação europeu Horizon 2020[10]. O LSP foi uma iniciativa de desenvolvimento da tecnologia IoT para a indústria e a sociedade em geral, através de programas de inserção de pilotos de IoT em larga escala em diferentes setores como mobilidade, agricultura e iluminação pública. Algumas entidades autônomas e stakeholders participaram de todo o processo, desde a criação do produto ou serviço e a fase de testes até a sua implementação e aplicação.[11]

---

regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

8. SAIIDI, Uptin. *What is a Smart City*? CNBC International. 2017. Disponível em https://www.cnbc.com/2017/02/09/how-smart-cities-are-building-the-future.html#:~:text=What%20is%20a%20smart%20city,many%20aspects%20of%20daily%20life
9. DUBAI NOW SMART APP disponível em https://www.bayut.com/mybayut/dubai-now-app/
10. EUROPEAN COMMISSION. SynchroniCity: *Delivering an IoT enabled Digital Single Market for Europe and Beyond* disponível em: https://cordis.europa.eu/project/id/732240
11. EUROPEAN COMMISSION. *Large Scale Pilots.* Disponível em: https://cordis.europa.eu/programme/id/H2020_IoT-01-2016

O LSP, de nome SynchroniCity, foi a primeira tentativa de criar um mercado digital único na Europa e pesquisou a capacidade das cidades inteligentes em potencializar a integração segura dos dispositivos em IoT, tornando-os interoperáveis para o compartilhamento de dados em aplicativos[12]. O programa envolveu vinte e uma cidades europeias entre elas Manchester, Milão, Porto e duas cidades da Coréia do Sul e contou com o apoio da Open & Agile Smart Cities Aliance[13], uma organização sem fins lucrativos com mais de 114 cidades participantes que tem a pretensão de criar um mercado aberto de cidades inteligentes baseado nas necessidades dos cidadãos.

Dentre os objetivos específicos do SynchroniCity estão a criação de serviços piloto de atendimento ao cidadão, a formulação de políticas, o planejamento das cidades e o estabelecimento de fundamentos técnicos de interoperabilidade mínimos. Inclusive, neste último objetivo citado, o SynchroniCity mostrou como os Mecanismos Mínimos de Interoperabilidade (MMIs) introduzidos pela rede Open & Agile Smart Cities (OASC) podem ajudar no mercado em IoT[14].

Todavia, antes de dar início à criação de produtos e serviços, o SynchroniCity realizou pesquisas e estudos sobre o mercado de dispositivos de IoT em smart city, uma vez que foi o primeiro LSP a abordar o tema. Assim, no próximo tópico, verificam-se as conclusões dessa importante etapa, antecessora à criação da rede única de IoT em smart city.

3. AS BARREIRAS DO MERCADO DIGITAL E AS PROPRIEDADES DA REDE ÚNICA DE *IOT* EM *SMART CITY*

O SynchroniCity investigou, nas cidades integrantes do LSP, os obstáculos que impedem ou dificultam a implantação em larga escala de dispositivos habilitados em IoT em tecnologia smart city. Foram encontrados 11 obstáculos, dos quais o projeto

12. EUROPEAN COMMISSION. *SynchroniCity. Delivering na IoT enabled Digital Single Marketfor Europe and Beyond.* Disponível em https://cordis.europa.eu/project/id/732240
13. OPEN AND AGILE SMART CITIES ALIANCE. Disponível em https://oascities.org/
14. OPEN AND AGILE SMART CITIES ALIANCE *Digital Interoperability: Big in Japan* Disponível em https://oascities.org/digital-interoperability-big-in-japan/

nomeou como "barreiras"[15]. Sete dessas barreiras foram classificadas como tecnológicas e as outras quatro como barreiras socioeconômicas.

As barreiras tecnológicas encontradas são a falta de padronização dos serviços e produtos dos fornecedores; a ausência de ambientes comuns para o fornecimento dos serviços nas cidades; a infraestrutura limitada de IoT; a ausência de ferramentas, modelos de licença de plataforma de compartilhamento de dados urbanos captados por dispositivos em IoT e outros conjuntos de dados relevantes; a carência de práticas comerciais harmonizadas e estruturas jurídicas nas cidades; a não compreensão das possíveis implicações dos serviços em IoT para a privacidade e a proteção dos dados pessoais e; a falta de confiança da população na adoção das tecnologias emergentes[16].

As barreiras socioeconômicas são os custos econômicos para a implantação da tecnologia e as restrições orçamentárias; as mudanças políticas frequentes e a falta de continuidade na implantação do projeto; a ausência de participação dos cidadãos e; a falta de uma estratégia para a implantação de uma cidade inteligente[17].

O SynchroniCity concluiu que essas barreiras fragmentam o mercado geral de smart cities o que prejudica a livre concorrência entre os fornecedores e a capacidade

15. GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. *Guidelines for SynchroniCity architecture* "*Identified barriers for the smart city market Our initial analysis in Section 2 reveals seven key technical and four socio-economic barriers that hamper the progress on the smart city market. technologies due to increasing technology fluidity Likewise, the key identified non-technical barriers included:* disponível em https://cordis.europa.eu/project/id/732240/results

16. GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. *Guidelines for SynchroniCity architecture. "Key identified technological barriers are: 1. Lack of standardized multi-vendor ecosystem 2. Lack of common service provisioning environments across cities 3. Close coupling of IoT infrastructure and applications (IoT solution silos) 4. Lack of tools, license models and platforms to facilitate the incentivized sharing of urban IoT data and other relevant data sets 5. Lack of harmonized business practice and legal frameworks across cities 6. Lack of understanding of privacy and personal data protection implications 7. Lack of confidence in adopting emerging"* (p. 2).

17. GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. *Guidelines for SynchroniCity architecture 1. Economical costs and budget constraints 2. Frequent political changes and lack of continuity 3. Lack of involvement of citizens, SMEs or support from them 4. Lack of a holistic smart city strategy*" (p. 2).

de formular soluções padronizadas para um grande mercado[18]. Visando eliminar essa fragmentação, o SynchroniCity buscou criar uma rede única e confiável para o desenvolvimento de produtos e serviços que utiliza a tecnologia IoT para smart city.

Para o projeto, este ambiente iria proporcionar um acesso facilitado para as empresas, as cidades e os cidadãos aos produtos e serviços habilitados em IoT nas zonas-piloto das cidades participantes do LSP, além de fornecer as condições adequadas para promover a competição e a inovação dos fornecedores sem afetar os direitos a proteção dos dados e a privacidade dos cidadãos. Os participantes do projeto acreditavam que esta rede única proveria o crescimento do mercado digital das cidades inteligentes.

Portanto, para desenvolver a rede única de IoT em smart city que atendesse às expectativas dos seus idealizadores, o SynchroniCity elaborou nove diretrizes, das quais deram o nome de "propriedades"[19]. Essas propriedades são características da rede única de IoT em smart city da SynchroniCity que foram pré-definidas pelo próprio programa. O projeto não esclareceu sobre uma possível hierarquia entre as propriedades ou se o programa priorizaria alguma propriedade em caso de conflito entre elas.

A primeira propriedade é a interoperabilidade. A cidade tem a liberdade de escolher, entre as opções de fornecedores, as camadas de tecnologia inseridas na plataforma e qual solução operacional deseja para os seus dispositivos em IoT.

Além disso, a interoperabilidade permite que as entidades administrativas, os cidadãos e as empresas troquem informações importantes para a transformação digital. Essa necessidade de interação é reconhecida pela União Europeia desde 1999, quando a interoperabilidade foi estipulada como um pré-requisito para ligações eficientes interfronteiras.

A European Interoperability Framework (EIF)[20] é um conjunto de

18. Idem, p. 11.
19. GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. *Guidelines for SynchroniCity architecture* disponível em https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b2ad5b30&appId=PPGMS (p. 12)
20. EUROPEAN COMMISION. *ISA² - Interoperability solutions for public administrations, businesses and citizens* disponível em https://ec.europa.eu/isa2/eif_en/

recomendações para a interoperabilidade de administrações, empresas e cidadãos criada pela União Europeia. A EIF trás orientações de configuração de serviços públicos digitais interoperáveis. Essa iniciativa visa melhorar a qualidade dos serviços públicos europeus através da interligação de serviços semelhantes entre os países, e incentivar uma legislação que não comprometa o desenvolvimento da interoperabilidade.

A segunda propriedade é a livre concorrência entre fornecedores de infraestrutura interoperável de IoT e entre provedores de soluções. Um ambiente digital aberto é propício para o desenvolvimento econômico e tecnológico.

Outra propriedade é o fornecimento de um único ambiente de serviço que promova a portabilidade dos dispositivos inteligentes. Os serviços urbanos implantados com sucesso em uma cidade podem ser instalados em outra, promovendo assim um mercado único digital. Isso permite a adaptação de interfaces de programação de aplicativos (APIs) que poderão obter fontes de dados equivalentes.

A quarta propriedade é a reutilização da infraestrutura de IoT. Os novos dispositivos inteligentes reutilizam a infraestrutura já instalada, uma vez que foram desenvolvidos no mesmo ambiente dos dispositivos antigos. Esta propriedade também gera grandes benefícios econômicos e sustentáveis.

A propriedade de número cinco é a confiança dos usuários nos provedores de serviços em IoT. Para isso, realizam-se acordos que garantem o uso responsável dos dados pessoais dos consumidores, haja vista a natureza aberta da rede em IoT.

A sexta propriedade é o compartilhamento grátis de dados que aumenta as oportunidades dos provedores e fornece um mercado livre. Já a propriedade de número sete é um ambiente jurídico comum que proporcione igualdade de condições em todas as zonas da plataforma.

Por fim, as propriedades oito e nove são, respectivamente, o aumento da competitividade e a criação de uma arquitetura que permita a participação de empresas de diversas cidades. Essas características incentivam a concorrência, gera empregos e aumenta a criação de produtos inovadores.

O programa procurou desenvolver uma estrutura distribuída, confiável e segura que permitisse o compartilhamento de informações heterogêneas para o uso de aplicativos em IoT nas cidades inteligentes. A criação de um mercado único de serviços

urbanos, habilitados em IoT por meio de um sistema integrado, contendo tanto consumidores como fornecedores, provedores de serviços e governos de diferentes cidades, favorece as ações corretivas, impedindo as violações no fluxo de dados.

Uma vez identificadas as dificuldades do mercado digital de smart cities e formuladas as características pretendidas pelo programa em uma rede única de IoT, o SynchroniCity deu início a fase de criação e desenvolvimento de sua rede. Assim, passa-se à sua análise.

4. A ARQUITETURA DA REDE SYNCHRONICITY

Para criar um ambiente digital em conformidade com as propriedades analisadas no tópico anterior, o projeto SynchroniCity elaborou uma estratégia de desenvolvimento de interoperabilidade dividida em três pilares. O primeiro é a troca de experiências na integração de várias implantações de IoT em cidades inteligentes. O desenvolvimento conjunto de uma mesma arquitetura favorece a padronização de uma estrutura aberta e interoperável.

O segundo pilar é a contribuição da Open & Agile Smart Cities Aliance, desenvolvedora de diretrizes para sistemas urbanos interoperáveis e responsável por implantar serviços em várias cidades. A OSCA forneceu uma plataforma que compartilha as melhores normas para implementação de smart city.

Por último, o terceiro pilar é o desenvolvimento de uma interface de programação de aplicativos aberta e interoperável para cidades inteligentes. A criação de uma API facilita o intercâmbio de dados para o desenvolvimento de novas tecnologias.

Na API existem dois atores, sendo um aquele que fornece os dados e o outro aquele que os utiliza. A maioria dos usuários de API está fornecendo e utilizando os dados. As empresas, por exemplo, acessam os dados para colher funcionalidades de outras entidades ou associações e expõe os seus dados para os seus clientes, parceiros e fornecedores.

Uma API baseada em um modelo de dados da OSCA oferece meios mais simples de consultar informações atualizadas da gestão de serviços de uma cidade. Caso sejam informações públicas, elas podem ser coletadas de aplicativos de terceiros. A integração entre sistemas e aplicativos de terceiros tem custo baixo.

A API SynchroniCity é portátil e interoperável. A sua diferença para outros projetos é a arquitetura única de serviços urbanos habilitados para IoT, que supera as barreiras socioeconômicas. A seguir, uma ilustração da sua estrutura:

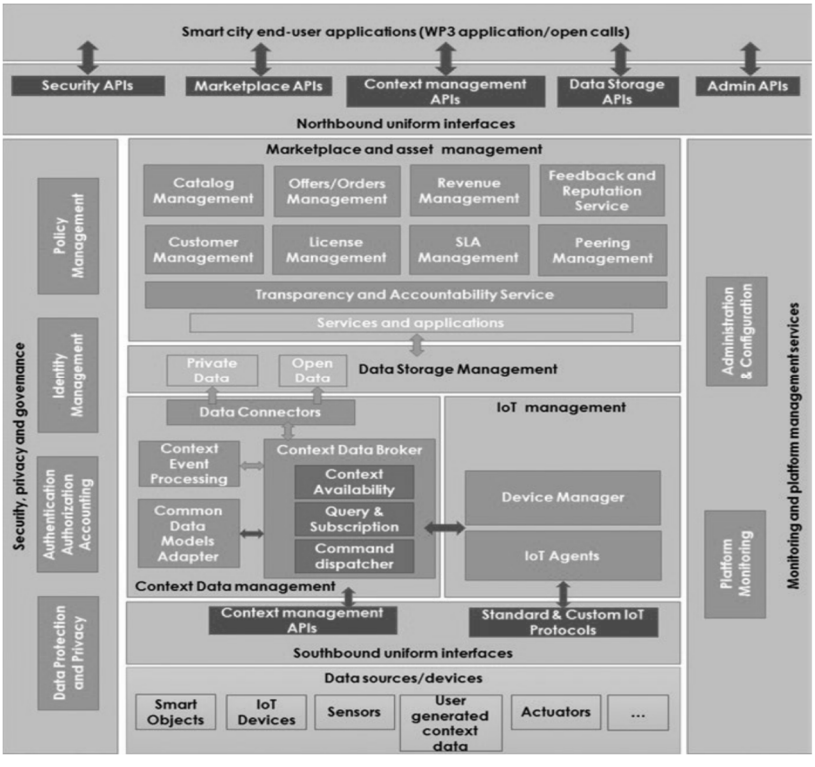


Figura 1. Arquitetura da SynchroniCity[21]

A arquitetura SynchroniCity tem como um dos seus componentes principais o *context data management*, que é uma espécie de software de comunicação de dados para aplicativos distribuídos. É responsável por conectar dois aplicativos que vão transmitir e compartilhar dados. [22]

O *context data management* é formado por quatro módulos, sendo o *context databroker*, o *context event processing,* o *common data models adapter* e o *data connector*. O *context databroker* é responsável por buscar os dados e colocá-los em uma interface padronizada. O *context event processing* analisa e responde um grande

21. ZIEGLER, Sébastien. *Internet of Things Security and Data Protection***.** Springer. 2019. Pg 161
22. AZURE. *O que é middleware ?* Disponível em https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-middleware/

número de transações. *common data models adapter* mapeia os dados heterogêneos para um modelo de dados pré-definido. Por fim, o *data connector* armazena os dados, criando um histórico[23].

Outro componente importante da arquitetura SynchroniCity é o *IoT management.* Ele permite que os dispositivos IoT enviem seus dados para o *context data management*, utilizando seus próprios protocolos. Em seguida, este software configura cada dispositivo de IoT para garantir uma boa conexão com os demais dispositivos.

O terceiro componente principal é o *data storage management*, responsável por armazenar todo tipo de dado em diferentes suportes como armazenamento local, plataforma de nuvem e banco de dados.

O quarto componente é o *Marketplace and asset managment*, que fornece bens e serviços às cidades inteligentes. Ele contém nove submódulos importantes que garantem as necessidades dos usuários. Um deles é o *transparency and accoutabillty service,* que é o responsável pela aplicação das preferências dos clientes relativa à proteção de dados pessoais. Este submódulo publica as finalidades e as restrições da coleta de dados em IoT.

A segurança, a privacidade e a governança são gerenciadas por vários submódulos. Um deles é o *data prottection and privacy que* visa garantir a confidencialidade, a integridade e a imutabilidade dos dados, por meio da criptografia. Há também um submódulo específico para gerenciamento de a identidade e de autenticação, outro submódulo para a autorização e a contabilidade da plataforma e um submódulo de gerenciamento de políticas usadas na plataforma SynchroniCity.

O último componente principal é o *platform management service*. Ele garante a administração e a configuração do SynchroniCity.

5. O SYNCHRONICITY E A ADEQUAÇÃO AO GDPR

Dois dos objetivos do SynchroniCity são a proteção dos dados pessoais e a adequação do seu projeto com o General Data Protection Regulation (GDPR), que é o regulamento europeu de normas relativas à proteção de dados das pessoas singulares e da sua livre circulação. Este diploma visa proteger os direitos e liberdades

23. ZIEGLER, Sébastien. *Internet of Things Security and Data Protection*. Springer. 2019, p. 161.

fundamentais, em especial o direito à proteção dos dados pessoais[24]

A política de dados do SynchroniCity promete cumprir as obrigações constantes no GDPR, entre elas a proteção proativa dos direitos dos titulares dos dados, a aplicação dos seus princípios basilares como a minimização de dados pessoais, a privacidade por design e por padrão, o investimento em pesquisas de otimização da proteção de dados nas cidades participantes e o accoutabillity[25].

Nesse sentido, o projeto desenvolveu uma estrutura de proteção de dados baseada em três eixos principais: I. Dois encarregados de proteção de dados (DPO) por cidade; II. A criação de uma ferramenta específica de Avaliação de Impacto de Proteção de Dados (DPIA) para cidades inteligentes; III. Um aplicativo de privacidade.

5.1. DOIS ENCARREGADOS DE PROTEÇÃO DE DADOS

Em resumo, o DPO (encarregado, no Brasil) é um intermediário entre as partes interessadas na proteção de dados, como os controladores, os titulares de dados a as autoridades governamentais. Sua principal função é auxiliar a conformidade do tratamento realizado pelo agente de tratamento de dados com a lei geral de proteção de dados, no caso, a GDPR.

Segundo o Guideline 243-2016 da união europeia, o DPO pode recolher informações para: identificar a atividade de tratamento; analisar e verificar a conformidade das atividades de tratamento e aconselhar, informar e recomendar o responsável pelo tratamento. Insta destacar que o DPO não responde pessoalmente pelo descumprimento da lei geral de proteção de dados[26].

No SynchroniCity ficou acordado que cada cidade seria um controlador e, por

24. GDPR "*Artigo 1º. Matéria e Objetivos 1. O presente regulamento estabelece regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e regras relativas à livre circulação de dados pessoais. 2. O presente regulamento protege os direitos e liberdades fundamentais das pessoas singulares e, em particular, o seu direito à proteção dos dados pessoais. 3.A livre circulação de dados pessoais na União não pode ser restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais*".
25. GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. *Guidelines for SynchroniCity architecture*, p. 56-57.
26. UNIÃO EUROPEIA – *WP9 Guideline* 243-2016, p. 20.

isso, seriam livres para determinar quais dados devem ser processados e como devem ser processados. Além disso, cada cidade deveria ter seu próprio DPO[27].

Para lidar com vários DPOs, a SynchroniCity nomeou um Coordenador de DPOs (CDPO), encarregado de supervisionar e coordenar o trabalho. Além disso, criou-se um Comitê de Proteção de Dados formado de vários DPOs para se reunirem regularmente e definirem a política de proteção de dados do projeto, coordenar os demais DPOs, atualizar a população sobre a proteção de dados do projeto e resolver problemas relativos à proteção de dados.

5.2. *PRIVACY BY DESIGN*

A SynchroniCity afirma que a sua Avaliação de Impacto e Proteção de Dados (DPIA) atende ao Privacy By Design, um dos conceitos mais importantes da privacidade dos dados, especificado no artigo 25 do GDPR[28] e no artigo 46 caput[29] e

27. ZIEGLER, Sébastien. *Internet of Things Security and Data Protection*. Springer. 2019 pg 164
28. UNIÃO EUROPEIA "GDPR "*Artigo 25. 1 Tendo em conta o estado da arte, o custo de implementação e a natureza, âmbito, contexto e finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares decorrentes do tratamento, o responsável pelo tratamento deve, tanto no momento da determinação dos meios de tratamento como no momento do próprio tratamento, implementar medidas técnicas e organizativas adequadas, como a pseudonimização, que visam implementar princípios de proteção de dados, como a minimização de dados, de forma eficaz forma e integrar as salvaguardas necessárias no tratamento para cumprir os requisitos do presente regulamento e proteger os direitos dos titulares dos dados.2O responsável pelo tratamento deve implementar as medidas técnicas e organizativas adequadas para assegurar que, por defeito, apenas sejam tratados os dados pessoais necessários para cada finalidade específica do tratamento. [2] Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao período do seu armazenamento e à sua acessibilidade. [3] Em particular, essas medidas devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados sem a intervenção do indivíduo a um número indefinido de pessoas singulares.3. Um mecanismo de certificação aprovado nos termos do artigo 42.º pode ser utilizado como elemento para demonstrar o cumprimento dos requisitos estabelecidos nos n.ºs 1 e 2 deste artigo*".
29. BRASIL. LGPD "*Artigo. 46 Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilíc*ito".

parágrafo 2º da Lei Geral de Proteção de Dados brasileira (LGPD) [30]. Tendo em vista a sua relevância, analisa-o antes de perquirir o DPIA.

O Privacy By Design, ou privacidade desde a concepção, significa que a privacidade e a proteção dos dados devem ser observadas desde a criação e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Esta concepção é alcançada através da aplicação dos sete Princípios Fundamentais, criados por Ann Cavoukian em 2009[31].

O primeiro princípio é o proativo, não reativo: preventivo, não corretivo. Defende a prevenção de eventos hostis à privacidade. Adotam-se práticas de proteção a privacidade antes que a violação dos dados ocorra.

A empresa de tecnologia da informação deve firmar e tornar público o seu compromisso na definição e cumprimento de altos padrões de privacidade. Além disso, deve se comprometer em adotar uma cultura de melhoria contínua da privacidade, estabelecer métodos para reconhecer práticas e projetos de privacidade inadequados e corrigir quaisquer impactos negativos antes deles ocorrerem.

O segundo princípio é a privacidade como padrão. O dispositivo em IoT deve estar configurado para oferecer o máximo grau de privacidade e garantir que os dados pessoais estejam protegidos automaticamente. A tecnologia deve proteger os dados mesmo que o titular não tome nenhuma medida protetiva.

Este princípio, também chamado de *Privacy By Default*, indica que o produto ou serviço, ao ser lançado no mercado, deve vir padronizado na configuração mais restrita possível de proteção e uso de dados. Desse modo, o dispositivo liberaria apenas à coleta de dados necessários para o seu funcionamento bem como o acesso mínimo desses dados por terceiros. Muitas empresas realizam o contrário do *Privacy By Default* e coletam o máximo de informações do usuário, embora permitam que o indivíduo desative essa configuração.

---

30. BRASIL. LGPD "*§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução*".
31. CAVOUKIAN, Ann. *Privacy By Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices.* Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://jpaulgibson.synology.me/ETHICS4EU-Brick-SmartPills-TeacherWebSite/SecondaryMaterial/pdfs/CavoukianETAL09.pdf

O terceiro princípio é a privacidade incorporada ao projeto. Toda arquitetura de sistema deve conter a privacidade desde o seu design, considerado-a um componente essencial de funcionalidade do seu núcleo. Este princípio minimiza o impacto da tecnologia sobre a privacidade, de forma que o uso indevido do dispositivo, um erro ou configuração incorreta não acarrete em vazamento de dados.

A incorporação da privacidade na tecnologia deve ser realizada de maneira holística, integrativa e criativa. Holística significa que a privacidade deve ser adotada de forma mais ampla possível, englobando todo o contexto do dispositivo. Já a maneira integrativa consiste em consultar todas as partes interessadas. Por fim, a maneira criativa é descobrir formas de prestar serviços ou reinventar produtos tecnológicos que sejam compatíveis com o princípio da privacidade. É importante que a empresa de tecnologia da informação adote padrões e frameworks reconhecidos pelo mercado.

O quarto princípio é a funcionalidade total que consiste em realizar todos os objetivos do projeto. A proteção à privacidade não pode significar perda de funcionalidade do dispositivo em IoT. Desse modo, o *privacy by design* defende que todos os objetivos devem ser alcançados, incluído a proteção à privacidade. Portanto, buscam-se soluções criativas capazes de agregar a maior quantidade de interesses possíveis, sejam eles protetivos ou funcionais.

Os criadores de dispositivos em IoT precisam valorizar a segurança das operações, pois ela gera valor econômico e será cada vez mais importante para a captação de clientes. Ressalta-se que a LGPD reconhece o desenvolvimento econômico e tecnológico inovador como um de seus fundamentos.

A segurança fim a fim é o quinto princípio fundamental e dispõe que a proteção dos dados pessoais deve ser realizada durante todo o ciclo de vida do dispositivo e não apenas em algum ponto específico do processo ou da arquitetura. Inicialmente, os produtos e serviços baseados em Internet of Things devem obedecer a três fundamentos da segurança[32], sendo eles a confidencialidade, a integridade e a disponibilidade.

32. DacNhuong Le e outros, definiram como: "*The CIA (Confidentiality, Integrity, Availability) triad is the unifying attribute for cybersecurity which is used to evaluate security of na organization using the three key areas related to security namely confidentiality, integrity and availability. These three attributes have specific requirements and operations.*" (p. 38).

A confidencialidade[33] significa manter uma informação conhecida somente para quem está autorizado. Promove o tráfego seguro de informações entre dispositivos. A sua violação tem como consequência o incidente mais conhecido que é o vazamento de dados pessoais, ou seja, a divulgação da informação sigilosa para terceiros não autorizados.

Divide-se o estudo da confidencialidade em duas óticas, quais sejam a dinâmica e a estática. A dimensão dinâmica se refere a confidencialidade durante o tráfego dos dados que ocorre entre dispositivos. Tem-se como exemplo o tráfego de dados pela internet de um servidor para o seu navegador.

Já a dimensão estática é a confidencialidade dos dados em repouso. Um exemplo é o armazenamento de dados em alguma mídia. Atualmente, o meio mais comum de proteção de confidencialidade de dados, seja em repouso ou em trânsito é a criptografia.

A integridade[34] é um fundamento que se refere ao dado que não pode ser

33. Moller definiu-a como: "*Confidentiality: Vital security characteristic in the era of digital transformation. Term is roughly equivalent to privacy. However, it means protecting data from unauthorized access and misuse, for instance by a set of rules that limit access to data. Measures undertaken to ensure confidentiality are designed to prevent sensitive data from reaching the wrong people, making sure that the right people can in fact get it. Federal Code 44 United States Code, Section 3542 defines confidentiality as "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information." This requires a number of access controls and protection as well as ongoing monitoring, testing and training. Data encryption is a common method of ensuring confidentiality. In this regard, user IDs and passwords constitute a standard procedure. Other options include biometric verification, by which a person can uniquely evaluate one or more distinguishing biological traits, as well as security token, which is a small hardware device that an owner carries to authorize access to a network service, and key fobs, which means a small, programmable hardware device that provides access to a physical object, or soft token, a software-based security token, that generates a single-use login PIN. However, to satisfy desired security requirements the solution should include a holistic consideration".* MOLLER, Dietmar P.F. *Cybersecurity in Digital Transformation Scope and Applications*. Editora Springler. Disponível: em https://link.springer.com/book/10.1007/978-3-030-60570-4, p. 30.

34. Moller definiu-a como "*Integrity: Involves maintaining consistency, accuracy, and trustworthiness of data over its entire life cycle. This covers the important topics of data integrity and system integrity. Data integrity is the requirement of data and programs being changed only in a specified and authorized manner, while system integrity refers to the requirement of a system performing its*

corrompido ou modificado por terceiros não autorizados. Uma técnica de verificação de integridade de dados é o hash, que é um número único, fruto de um cálculo realizado por algoritmos, que identifica aquele pacote de dados. Se o hash for modificado, tem-se a confirmação de que aquele pacote de dados foi alterado, comprometendo a sua informação original.

O fundamento da disponibilidade[35] consiste em ter o dado, serviço ou produto quando o usuário deseja. É a garantia de que o sistema estará disponível o máximo de tempo possível.

O próximo princípio fundamental é a visibilidade e transparência que constitui na garantia de verificação pelos usuários de que a tecnologia está operando em conformidade com os princípios do *privacy by design* e com os seus objetivos funcionais. É importante a criação de mecanismos de reclamação e reparação, além de disponibilizar informações claras e objetivas sobre a utilização do produto ou serviço.

Por último, tem-se o respeito pela privacidade do usuário, do qual impõe aos arquitetos e operadores que trabalhem de acordo com o interesse do indivíduo, desenvolvendo dispositivos seguros. O *Privacy By Design* coloca o usuário no centro do produto ou serviço que deve ser desenvolvido com base nos seus interesses.

---

intended function in na unimpaired manner, free from deliberate or inadvertent unauthorized manipulation. Against this background, a deficiency in integrity can allow for modification of data and programs stored on the memory of digital systems used, which can affect the crucial and critical operational functions of the digital systems, without ad hoc detection". Idem, p. 30.

35. Moller definiu-a como "*Availability: Information, data and programs are accessible by authorized users when needed and is an essential requirement in the era of digital transformation. This can be ensured by rigorously maintaining all system hardware, immediately performing hardware repairs when needed, and maintaining a correct functioning operating system environment that is free of software conflicts. If crucial and critical operational systems cannot access needed data When required, data, and programs of operational systems are not secure. That availability is a fundamental feature of a successful deployment of digital systems in the era of digital transformation. To prevent data loss, a backup copy may be stored in a geographically isolated location, perhaps even in a digital safeguard. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data and programs due to malicious activities such as Denial-of-Service attacks, and network intrusions".* Idem, p. 30-31.

5.3. AVALIAÇÃO DE IMPACTO E PROTEÇÃO DE DADOS (DPIA) PARA *SMART CITY*

A Avaliação de Impacto e Proteção de Dados é um processo formal que objetiva identificar e avaliar riscos de privacidade no projeto, política, programa, serviço ou produto e encontrar soluções para evitar ou mitigar esses riscos[36]. O DPIA é realizado antes do início do tratamento dos dados.

O artigo 35 do GDPR[37] dispõe que a DPIA é obrigatória quando for utilizada uma nova tecnologia no tratamento de dados e se a natureza, o contexto ou a finalidade do tratamento puderem resultar num elevado risco para os direitos e liberdades das pessoas. No caso do SynchroniCity, entende-se que a confecção do DPIA é obrigatória pois adota nova tecnologia e monitora grandes áreas de espaço público. Desse modo, foi acordado que todas as cidades envolvidas com o projeto teriam que criar seu próprio DPIA e se declararem autoridades locais.

---

36. Conceito de Avaliação de impacto e Proteção de Dados na LGPD "*artigo 5º inciso XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.*" Para o GDPR, o DPIA: (84) "*A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais*".
37. GDPR "*Artigo 35. Avaliação do impacto da proteção de dados. 1 Sempre que um tipo de tratamento, em particular que utilize novas tecnologias, e tendo em conta a natureza, âmbito, contexto e finalidades do tratamento, possa resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve, previamente ao tratamento, proceder a uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais. 2 Uma única avaliação pode abordar um conjunto de operações de processamento semelhantes que apresentam riscos elevados semelhantes*".

Esta medida beneficiou o projeto, pois reduziu a responsabilidade da aplicação da lei da supervisão, melhorou o processo local de tomada de decisão em matéria de proteção de dados, aumentou a conscientização sobre a privacidade nos órgãos de cada cidade e reforçou a confiança dos usuários nos processamentos dos seus dados. A DPIA da SynchroniCity foi projetada e adaptada para abordar as necessidades e riscos potenciais relacionados a implantação da IoT no ambiente urbano.

Foi estabelecido que a DPIA de cada cidade mapearia os riscos, forneceria contramedidas e ajudaria a projetar a cidade inteligente de acordo com os princípios da privacidade e proteção de dados[38]. Desse modo, cada cidade deveria identificar o alvo de avaliação da DPIA em smart city, que poderia ser vários componentes como sistema de sensores, câmeras, interfaces, banco de dados ou um serviço de gestão de tráfego eficiente. Essa questão foi tratada pelo DPO da cidade conjuntamente com o DPOC.

Ao realizar uma DPIA, foram chamados os stakeholders que são todas as partes interessadas que serão autorizadas a acessar e explorar os dados pessoais. Consideram-se interessados em uma DPIA de smart city a cidade, representada pelo órgão governamental, os seus cidadãos, as empresas que prestam serviços públicos, os operadores e provedores de serviços, as universidades, os desenvolvedores de aplicativos e empresas de pesquisa em marketing e segmentação de cliente[39].Com a exceção dos cidadãos, todas as entidades acima mencionadas podem ser controladoras ou processadoras de dados.

Além disso, a DPIA deveria ter setores estratégicos como coordenadores de projeto, diretores jurídicos de avaliação de conformidade com a GDPR e Engenheiros de Tecnologia da Informação e Comunicação (TIC) para avaliarem soluções de cidades inteligentes. Para garantir a uniformidade do processo, todas as atividades seriam coordenadas pelo DPO da respectiva smart city.

Depois de identificados os riscos e as medidas cabíveis, o DPO chegaria a sua conclusão. Caso o resultado da DPIA mostrasse um risco baixo para o titular dos dados, então o DPO declarava que o projeto era aceitável. Desse modo, é estabelecido um

38. GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo et al. *Guidelines for SynchroniCity architecture*, p. 10.

39. Idem, p. 163.

plano de ação com atribuição de recursos, prazos e responsabilidades para a implementação das contra medidas. Porém, se o DPIA identificasse alto risco, o DPO não considerava o projeto aceitável. Nesse caso, o DPO suspenderia o projeto e consultaria o seu supervisor.

5.4. APLICATIVO DE PRIVACIDADE

O Privacy App[40], aplicativo desenvolvido pelo projeto SynchroniCity, ficou disponível de forma gratuita e em vários idiomas em smartphone, Android e iPhone, e permitia que cidades inteligentes compartilhassem informações sobre todos os dispositivos IoT implantados. O objetivo do aplicativo era informar os cidadãos sobre a implantação da IoT em cidades inteligentes e o processamento dos dados. Após noticiar o cidadão, o aplicativo pedia o seu consentimento para coletar os seus dados pessoais.

O acesso às informações era através de um mapa interativo que exibia as localizações de cada dispositivo IoT em smart city, permitindo a ciência do cidadão sobre a existência de cada dispositivo.

Cada ícone do mapa representava um dispositivo em IoT e possuia informações detalhadas sobre ele, como a finalidade da coleta dos dados, o período de retenção dos dados, quem pode acessá-los e o controlador. Além disso, permitia que o titular dos dados entrasse em contato com o controlador e que o cidadão identificasse qualquer dispositivo IoT que ainda não estava no mapa do programa.

6. CONSIDERAÇÕES FINAIS

Buscou-se no presente estudo, em linhas gerais, identificar os problemas atuais para a implantação dos dispositivos de IoT em smart city, especialmente os problemas técnicos e jurídicos referentes a privacidade e a proteção de dados pessoais.

Como referência principal, estudou-se o projeto SynchroniCity, suas propriedades para uma rede de dispositivos de IoT em smart cities, seu modelo de arquitetura para um mercado único digital de serviços urbanos habilitados para IoT e as soluções

40. Disponível em: https://www.privacyapp.info/

nele encontradas para a privacidade e a proteção dos dados dos usuários.

Também foram analisados o *Privacy By Design*, conceito basilar do GDPR e da LGPD, bem como as medidas adotadas pelo projeto SynchroniCity para se adequar ao GDPR como a nomeação de DPOs, a criação da Avaliação de Impacto e Proteção de Dados para smart cities e o desenvolvimento de um aplicativo de privacidade.

A partir da pesquisa bibliográfica realizada, foi possível jogar luz sobre alguns dos principais pontos problemáticos que circundam o tema, dentre os quais a dificuldade de padronização dos dispositivos em IoT, a ausência de interoperabilidade dos dispositivos de IoT em smart cities, os obstáculos para a conformidade da arquitetura em IoT com a legislação de privacidade e proteção de dados e a ausência de estratégia para a implantação de medidas de proteção de dados em programas de implantação de IoT em smart cities.

REFERÊNCIAS

AZURE. *O que é middleware***?** Microsoft. Disponível em https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-middleware/ acesso em 06.07.2022

BRASIL, Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais***.** de 11 de maio 2016. Diário Oficial da União. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em 27.06. 2022

BRASIL. *LGPD. Guia de boas práticas 2020.* Agosto 2020. Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf Acesso em 01.07.2022

CAVOUKIAN, Ann. *Privacy By Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices.* Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://jpaulgibson.synology.me/ETHICS4EU-Brick-SmartPills-TeacherWebSite/SecondaryMaterial/pdfs/CavoukianETAL09.pdf Acesso em 09.01.2023

DUBAI NOW SMART APP disponível em: https://www.bayut.com/mybayut/dubai-now-app/ Acesso em 01.07.2022

EUROPEAN COMMISION *European Interoperability Framework – Implementation Strategy* disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:134:FIN Acesso em 05.07.2022

EUROPA COMMISSION. *Guideline 243-2016- DPO.* Disponível em https://ec.europa.eu/info/law/law-topic/data-protection_en abril de 2017 Acesso em 20.06.2022

EUROPEAN COMMISION. *ISA² - Interoperability solutions for public administrations, businesses and citizens* disponível em https://ec.europa.eu/isa2/eif_en/ Acesso em 02.07.2022

EUROPEAN COMMISSION. *Large Scale Pilots.* Disponível em: https://cordis.europa.eu/programme/id/H2020_IoT-01-2016 Acesso em 20.12.2022

EUROPEAN COMMISSION. *Smarts Cities. Cities using technological solutions to improve the management and efficiency of the urban environment***.** https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en Acesso em 05.07.2022

EUROPEAN COMMISSION. *SynchroniCity. Delivering na IoT enabled Digital Single Marketfor Europe and Beyond.* Disponível em: https://cordis.europa.eu/project/id/732240 Acesso em 15.06.2022

EUROPEAN COMMISSION. *Towards a Just and clean urban transition***.** Disponível em: https://smart-cities-marketplace.ec.europa.eu/ Acesso em 05.07.2022

GLUHAK, Alex, GAGLIONE, Alex, CAPOSSELE, Angelo e OUTROS. *Guidelines for SynchroniCity architecture* disponível em https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b2ad5b30&appId=PPGMS Acesso em 10.07.2022

INTERNATIONAL TELECOMMUNICATION UNION. *Smart sustainable cites: Na analysis of definitions.* Focus Group Technical Report. 2014.

IQBAL, Muhammad Azhar, HUSSAIN, Sajjad, XING, Huanlai, Imran, Muhammad Ali. *Enabling the Internet of Things: Fundamentals, Design, and Apliccations.*. Editora John Wiley & Sons Ltda. Primeira edição. 2021.

JARA. Antonio J. BOCCHI, Yann e outros. *An Analysis of Context-Aware Data Models for Smart Cities: towards fiware and etsi cim emerging data model* disponível em https://www.int-arch-photogramm-remote-sens-spatial-inf-sci.net/XLII-4-W3/43/2017/isprs-archives-XLII-4-W3-43-2017.pdf 2017 Acesso em 02.07.2022

JARA. Antonio J. BOCCHI, Yann e outros. *Smart Cties Semantics and Data Models*. Springer 2018

LARRIEUX, Aurelia Tamò. *Designing for Privacy and its Legal Framework***.** Data Protetction by Design and Defautl for Internet of Things. Springer. 2018.

LE, DacNhuong, e outros. *Cyber Security in Parallel and Distributed Computing. Concepts, Techniques, Applications and Case Studies.* John Wiley & Sons, Inc. 2019.

MEDDEB, Riad, HANDFORTH, Calum. *Necesitamos ciudades más inteligentes, no "smart cities".* MIT Tecnology Review. jun. 2022. Disponível em: https://www.technologyreview.es/s/14329/necesitamos-ciudades-mas-inteligentes-no-smart-cities Acesso em 02.07.2022

MOLLER, Dietmar P.F. *Cybersecurity in Digital Transformation Scope and Applications.* Editora Springler. Disponível: em <https://link.springer.com/book/10.1007/978-3-030-60570-4> . 2020. Acesso em 09.01.2023

MORAES, Alexandre de; HAYASHI, Vitor Takashi. *Segurança em Iot. Entendendo os riscos e ameaças em Internet das Coisas*. Editora Alta Books. 2021.

OLIVEIRA, Sérgio de. *INTERNET das COISAS com ESP8266, ARDUINO e RASPBERRY P1.* Editora Novatec LTDA. Junho/2017 primeira edição.

OPEN AND AGILE SMART CITIES ALIANCE *Digital Interoperability: Big in Japan* Disponível em https://oascities.org/digital-interoperability-big-in-japan/ Acesso em 07.06.2022

PARENTONI, Leonardo. *Compartilhamento de Dados Pessoais e a Figura do Controlador*. 2021. Disponível em https://www.researchgate.net/profile/Leonardo-Parentoni Acesso em 29.06.2022

PRIVACYAPP. Disponível em https://www.privacyapp.info/ acesso em 08.07.2022

QUALCOMM. *Smart Cities. Connecting the cities of the future*. Disponível em: https://www.qualcomm.com/products/application/smart-cities Acesso em 03. 07. 2022

SAIIDI, Uptin. *What is a Smart City?* CNBC International. **2017.** Disponível em https://www.cnbc.com/2017/02/09/how-smart-cities-are-building-the-future.html#:~:text=What%20is%20a%20smart%20city,many%20aspects%20of%20daily%20life.

UNIÃO EUROPEIA. *General Data Protection Regulation*. Disponível em https://gdpr-info.eu/ Acesso em 02.07.2022

ZIEGLER, Sébastien. *Internet of Things Security and Data Protection***.** Springer. 2019

ZIOSI, Marta; HEWITT, Benjamin; JUNEJA, Prathm; TADDEO, Mariarosaria; FLORIDI, Luciano, Smart Cities: Reviewing the Debate about their Ethical Implications (January 5, 2022). Disponível em SSRN: https://ssrn.com/abstract=4001761 ou http://dx.doi.org/10.2139/ssrn.4001761 Acesso em 05/01/2023.

O INEDITISMO DOS DISPOSITIVOS IOT E SUA RELAÇÃO COM O PARADOXO DA PRIVACIDADE

Júlia Lio Rocha Camargo

Mestranda em Direito, Tecnologia e Inovação pela UFMG. Pós-graduada em Compliance, Ética e Governança Corporativa pela PUC Minas. Bacharel em Direito. Professora Auxiliar de Pós-Graduação na PUC Minas. Advogada Corporativa.

DOI: https://doi.org/10.59224/dti5.ch11

Resumo: Em síntese, o presente artigo tem como objetivo compreender e estudar a configuração do *privacy paradox* e sua relação com a mais recente tecnologia: a Internet das Coisas. Neste trabalho, será analisado "se" e "de que forma" os dispositivos *IoT* ampliam o debate decorrente desse fenômeno, bem como quais seriam as medidas possíveis de serem aplicáveis para mitigar essa controvérsia.

Palavras-chave: *Privacy Paradox*; Privacidade; e Internet das Coisas (*IoT*).

Abstract: *In summary, this article aims to analyse and study the configuration of the privacy paradox and its relation with the latest technology: the Internet of Things. This paper will analyze "if" and "how" IoT devices expand the debate about this phenomenon, and what would be the possible measures that could be applied to mitigate this controversy.*

Keywords: *Privacy Paradox; Privacy; and Internet of Things (IoT).*

1. INTRODUÇÃO

A popular definição de privacidade desde os tempos modernos decorre da famosa

expressão "*direito de ser deixado só*"[1]. Essa frase, muito difundida pelo trabalho de Warren e Brandeis no século XIX, foi utilizada quando iniciaram os questionamentos sobre veiculação na impressa de imagens de terceiros nos meios de comunicação sem sua expressa autorização.

As máquinas fotográficas – que foram uma recente inovação da época – estavam se popularizando na sociedade, mas seu uso já despertava certo receio entre os indivíduos, que se viam preocupados com a utilização indiscriminada dessa nova tecnologia que poderia expor ao conhecimento público os aspectos de sua vida privada. A preocupação que se instaurava era de que "*o advento de novas tecnologias estavam expondo aspectos da vida privada, contra a vontade das pessoas, muitas vezes com o intuito comercial de lucro*"[2].

Apesar do contexto aqui narrado nos remontar a acontecimentos ocorridos em uma época muito distinta da atual, fato é que o questionamento levantado por tais pesquisadores poderia ser facilmente aplicável para várias das tecnologias atuais, as quais, algumas vezes, trabalham com aspectos da vida privada de um indivíduo sem sua efetiva ciência (ou sem que este tenha noção da real complexidade do uso de seus dados). Basta imaginar o histórico de compras de determinado indivíduo em uma empresa de varejo: esses dados são armazenados em provedores de nuvem localizados no país X, tratados por desenvolvedores e cientistas de dados do país Y, para que a empresa possa, então, fornecer seus serviços e produtos no país Z.

Conforme será apresentado neste artigo, as pesquisas indicam que esse desassossego da privacidade dos usuários em razão da aplicação de novas tecnologias não diminuiu. Os indivíduos estão genuinamente preocupados com o tratamento massivo de seus dados no ambiente *online* e o risco de vazamento de suas informações a terceiros.

Por outro lado, também será discutido que esses mesmos usuários – deliberadamente – optam, muitas vezes, por não se atentar as regras e políticas aplicáveis ao

1. WARREN, Samuel; BRANDEIS, Louis. *The Right to Privacy*. Harvard Law Review. Cambridge. Harvard University Press. v. IV, n. 05, p. 193-217, Dec. 1890. p. 194.
2. PARENTONI, Leonardo. O Direito ao Esquecimento (Right to Oblivion). In: DE LUCCA, Newton et al. *Direito & Internet III*: Marco Civil da Internet (Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015, p. 540.

tratamento dos dados pessoais ali cedidos para a contratação de produtos e serviços de seu interesse.

Essa contradição é o que define o "*privacy paradox*", conceito utilizado para sintetizar a situação de que "os indivíduos alegam que valorizam sua privacidade, mas não parecem agir de acordo"[3] (tradução livre).

Dentro desse contexto, um grande ponto de discussão na doutrina tem sido os riscos na utilização dos chamados "dispositivos inteligentes" (neste trabalho referenciados simplesmente como "*IoTs*"). Isso porque, os *IoTs* permitem uma coleta massiva de dados, em quantidade de armazenamento e tratamento de forma inédita e diferente de qualquer outra tecnologia, a qual, a depender de seu uso e aplicação, poderia gerar riscos de privacidade ainda pouco conhecidos ao usuário. Ao mesmo tempo, tais dispositivos já se mostraram extremamente relevantes e eficientes aos indivíduos, com um espectro de aplicação extremamente amplo: há dispositivos inteligentes para ajustar a temperatura de determinados ambientes[4], para proporcionar conforto e redução de gastos, assim como há apetrechos que podem ser utilizados em tratamentos médicos menos invasivos e onerosos aos pacientes[5].

Nesse sentido, o presente trabalho terá como objetivo descrever brevemente ao leitor as discussões sobre o tema, analisando "se" e, em caso positivo, "de que forma" essa recente inovação tecnológica se relaciona com o debate sobre o *privacy paradox* e quais os impactos relacionados a privacidade.

2. "*PRIVACY PARADOX*": CONCEITO E CONTEXTO

É fato que a *internet* alterou a forma como consumimos produtos e serviços a

3. WILLIAMS, Meredydd; NURSE, Jason; CREESE, Sadie. *The Perfect Storm: The Privacy Paradox and the Internet-of-Things*. University of Oxford, 2018a, p. 01. Disponível em: https://ieeexplore.ieee.org/abstract/document/7784629#citations. Acesso em: 03 jul. 2022.
4. ROVAI, Marcelo. *O IoT feito simples: Monitorando a temperatura desde qualquer lugar*. Disponível em: https://mjrobot.org/2017/01/06/o-iot-feito-simples-monitorando-a-temperatura-desde-qualquer-lugar/. Acesso em: 08 jul. 2022.
5. IOT NA MEDICINA: COMO FUNCIONA E EXEMPLOS. Folha Tecno. Disponível em: **https://www.folhatecno.com.br/2021/10/iot-medicina-como-funciona.html**. Acesso em: 05 jul. 2022.

partir de aplicações via *web*, plataformas e, até mais recentemente, com os objetos ditos "inteligentes", os *IoTs*, que coletam informações do "mundo físico", sem necessariamente a interação ativa de um usuário. Essas novas ferramentas têm como diferencial a geração, coleta, processamento e compartilhamento de dados em larga escala, sendo o estudo e análise de tais interações ferramenta indispensável para a atividade de empresas no mundo conectado.

A partir de um maior volume e variedade, de informações, aliado a um aumento da capacidade de processamento e conjugação dos dados, com rapidez, as empresas puderam aprender – e seguem aprendendo – sobre o perfil dos usuários: suas preferências, conceitos de compra e comportamento na rede. Com esse grande volume de dados, as plataformas conhecem o perfil de seus consumidores, tendências de compra, adequação de preço dos produtos e até como ajustar erros de usabilidade em suas próprias ferramentas.

O fato é que o poder transformador dessa economia é baseado em dados pessoais, os quais são coletadas sem a efetiva ciência do usuário em grande parte das vezes[6]. Tal conduta ainda que praticada dentro dos limites da lei, pode resultar em situações de violação ao direito da privacidade, e, consequentemente, de sua liberdade e da autodeterminação do indivíduo[7]. O controle do indivíduo sobre seus dados pessoais não é baseado apenas em consentimento, mas em conhecimento sobre a coleta e tratamento destes, conforme será abordado neste trabalho[8].

É a partir desse cenário que o conceito de privacidade foi atualizado e passou a ser melhor definido como "*direito do indivíduo de ser deixado só, adquirindo*

6. Sobre o tema Gabriela Monteiro explica que: "É que, conquanto o fornecimento de dados pessoais seja do conhecimento e desejado pelo cliente em muitos casos, em outros, a varredura, a coleta e a utilização de dados do usuário ocorrem sem a sua autorização ou mesmo sem o seu conhecimento." MONTEIRO, Gabriela Reis Paiva. *Big data e concorrência: uma avaliação dos impactos da exploração do big data para o método antitruste tradicional de análise das concentrações econômicas*, 2017. Dissertação (Mestrado em Direito) – Escola de Direito Getúlio Vargas, Rio de Janeiro, p. 10).
7. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 117.
8. Apenas a título explicativo, na opinião desta autora, a exigência de consentimento expresso e tradicional não seria compatível com muitas das tecnologias atuais, as quais se fundamenta em decisões automatizadas e algoritmos.

progressivamente um caráter mais positivo, como sendo o direito de se construir uma esfera privada própria" [9]. Isso significa, que o indivíduo tem a garantia de não ter os aspectos de sua vida privada interferidos e/ou influenciados a partir da atuação da tecnologia, salvo quando decorrentes de produtos e serviços expressamente contratados por este.

É justamente por isso que, considerando o atual cenário de uma sociedade datificada, a privacidade não é mais uma questão apenas de sigilo, esse conceito também está conectado com a capacidade de um indivíduo controlar a circulação e transação de informações sobre si mesmo, bem como influenciar de maneira efetiva a coleta, armazenamento e uso de suas informações.

Não por acaso, é possível perceber que os usuários estão interessados e se preocupam com sua privacidade. Um estudo de 2015, conduzido por pesquisadores da Escola de Comunicação da Universidade da Pensilvânia, em conjunto com o Instituto de Pesquisas de Princeton, indicou que 84% (oitenta e quatro por cento) dos entrevistados querem ter o controle sobre o que profissionais de *marketing* podem aprender sobre os usuários *online*[10]. Também revelou que 91% (noventa e um por cento) dos usuários questionados não concorda que *"se as empresas oferecem desconto, é uma troca justa que eles possam coletar informações sobre mim sem que eu saiba"*[11].

O curioso é que ao mesmo tempo que os usuários demonstram uma preocupação com a segurança e privacidade de seus dados na *internet*, a conduta destes aponta, muitas vezes, para o sentido contrário. Esse é o *privacy paradox*.

Um estudo feito pela Comissão Europeia, em 2016, revelou que apenas 9% dos

9. MENDES, Laura Schertel. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. 2008, p. 10. f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2008. Disponível em: https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf. Acesso: 16 set. 2022.
10. TUROW, Joseph; HENNESSY, Michael; DRAPER, Nora. *The Tradeoff F adeoff Fallacy - How Marketers Ar eters Are Misrepresenting esenting American Consumers and Opening Them up to Exploitation*. University of Pennsyvania, 2015, p. 3-4. Disponível em: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1554&hx0026;context=asc_papers. Acesso em: 05 jul. 2022.
11. No original: *"If companies give me a discount, it is a fair exchange for them to collect information about me without my knowing."* (Ibid, p. 3-4).

usuários acessam o endereço eletrônico no qual os termos e condições de produtos e serviços estão disponíveis[12]. Isso significa que, quase 90% (noventa por cento) dos usuários entrevistados aceitam as regras impostas por empresas para produtos e serviços de seu interesse sem sequer dispender tempo para compreender o básico das regras aplicáveis. Essa configuração é no mínimo contraditória com o desejo dos usuários de possuir o controle sobre o que acontece com seus dados pessoais.

Não por acaso, uma outra pesquisa apresentada na 22ª Conferência Internacional da *World Wide Web*, feita em 2013, identificou que os usuários estavam dispostos a comercializar o histórico de acesso das suas pesquisas no *browser* por 2 (duas) semanas pelo valor de €7 (sete euros) – o que inclusive foi ironizado pelos autores com a expressão "*o histórico do seu browser por um big mac*"[13]. Mais surpreendente, foi a pesquisa ter revelado que os usuários valorizam ainda mais seus dados *offline*, como idade e endereço, pois o preço de tais informações não eram comercializadas por menos de €25 (vinte e cinco euros).

Nesse sentido, visando identificar a diferença entre a intenção dos usuários em promover a proteção de seus dados pessoais ("*privacy intencion*") e o seu real comportamento ("*privacy behaviour*")[14], foi feito um experimento com usuários que realizam compras *online* em determinada loja de departamento[15]. Inicialmente, os participantes eram questionados sobre aspectos ligados à sua privacidade e proteção de dados pessoais, para posteriormente iniciarem suas compras, virtual. Ao longo da

12. COMISSÃO EUROPEIA. *Study on consumers' attitudes towards Terms and Conditions (T&Cs)*, 2016, p. 11. Disponível em: https://ec.europa.eu/info/sites/default/files/terms_and_conditions_final_report_en.pdf. Acesso em: 05 jul 2022
13. CARRASCAL, Juan Pablo; RIEDERER, Christopher; ERRAMILLI, Vijay; e CHERUBINI, Mauro. *Your browsing behavior for a big mac: Economics of personal information online*, in 22nd International Conference on World Wide Web, 2013, pp. 189–200.
14. KOKOLAKIS, Spyros. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Dept. of Information & Communication Systems Engineering, University of the Aegean, 2015, p. 4. Disponível em: https://www.researchgate.net/publication/280244291. Acesso em: 08 jul. 2022.
15. SPIEKERMANN, Sarah; GROSSKLAGS, Jens; BERENDT, Bettina. E-privacy in 2nd Generation ECommerce: Privacy Preferences versus actual Behavior, 2001. Disponível em: https://www.researchgate.net/publication/2480871_E-privacy_in_2nd_Generation_E-Commerce_Privacy_Preferences_Versus_actual_Behavior. Acesso em: 08 jul. 2022.

interação com a loja *online*, os usuários eram incentivados a conversar com um "robô 3D", sendo perceptível que os usuários revelavam mais informações ao assistente virtual que durante a interação com atendentes humanos, respondendo inclusive perguntas muito pessoais, contextualizadas por meio de engenharia social.

É justamente diante desse cenário conflituoso, o qual se caracteriza pela dicotomia entre o posicionamento dos usuários sobre a proteção de seus dados e seu efetivo comportamento, que se configura o "*privacy paradox*"[16]. Esse conceito inclusive já foi discutido internacionalmente em âmbito judicial, tendo o tribunal alemão definido como sendo a contradição "*entre a preocupação dos usuários da Internet sobre a proteção inadequada de sua privacidade na Internet e um tratamento genuinamente descuidado de seus próprios dados pessoais na Internet*"[17].

Neste ponto, é sempre importante considerar a premissa de que o usuário não é capaz de agir de forma racional quando comparado com demais agentes do mercado, no que diz respeito aos seus dados pessoais e a sua privacidade[18]. Conforme destacado pelo autor Spyros Kokolakis (2015), essas decisões de comportamento dos usuários, aparentemente descuidadas, seriam baseadas em informações incompletas e racionalidade limitada dos indivíduos, os quais muitas vezes não possuem o conhecimento técnico suficiente para compreender as consequências daquela decisão.

O *privacy behaviour* também tem uma explicação baseada na economia comportamental[19]. Um estudo feito para entender as inconsistências do comportamento dos usuários indica que estes possuem vieses relacionados a gratificação imediata, ou

16. KOKOLAKIS, 2015, *op. cit.,* p. 5.

17. No original: *"[...] between the concern of Internet users about inadequate protection of their privacy on the Internet and a genuinely careless handling of their own personal data on the Internet"* (ALEMANHA. High Court of Dusseldorf. Caso V1-Kart 1/19, 26 de agosto de 2019, p. 25.

18. KOKOLAKIS, 2015, *op. cit.,* p. 4.

19. Sobre o tema: "Analisar que as pessoas não querem pagar por privacidade ou não se importam com privacidade, portanto, é apenas uma meia verdade. As pessoas podem não ser capazes de agir como agentes economicamente racionais quando se trata de sua privacidade". No original: *"Observing that people do not want to pay for privacy or do not care about privacy, therefore, is only a half truth. People may not be able to act as economically rational agents when it comes to personal privacy"*. (ACQUISTI, Alessandro. Privacy in electronic commerce and the economics of immediate gratification, 2004. Disponível em: https://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf. Acesso em: 09 jul. 2022).

seja, que o indivíduo tende a valorizar os benefícios presentes mais do que os futuros riscos[20]. Não menos relevante, outro viés ao qual os indivíduos também são *submetidos, é o de seria impossível se proteger de toda e qualquer invasão de sua privacidade, por isso "eles podem não estar dispostos a adotar uma estratégia de proteção da privacidade de forma rígida, uma vez que eles duvidam que isso valerá a pena"* (tradução livre)[21].

O que se percebe é, então, que os indivíduos, ao tomar decisões sobre o compartilhamento de seus dados pessoais, por exemplo, não conseguem calcular os riscos e benefícios, de fato, envolvidos naquela operação. Estes não possuem todas as informações necessárias para chegar a uma conclusão bem-informada: suas decisões são feitas em tempo limitado e com assimetria de informação.

Essa discussão sobre a consciência dos usuários ao tomar decisões arriscadas, nas quais não é possível tangibilizar os riscos e benefícios facilmente, é tema para toda uma pesquisa – a qual, inclusive, já levou pesquisadores como o psicólogo Daniel Kahneman a ganhar o prêmio nobel da Economia em 2002[22]. Contudo, para fins da análise do fenômeno do *privacy paradox* abordado neste trabalho, é importante que o leitor tenha ciência sobre as muitas fragilidades do conceito sobre envolvido no comportamento "aparentemente" descuidado dos usuários na rede. Isso porque tal premissa compreende o usuário como um ser racional e que sempre busca a maximização de suas escolhas, o que não necessariamente ocorre em razão de explicações psicológicas e comportamentais.

3. A CONFIGURAÇÃO DO *PRIVACY PARADOX*

Não há dúvidas sobre a necessidade de estudo e aprofundamento no tema do *privacy paradox*, em especial para a adoção de medidas que tenham como o objetivo a proteção dos dados pessoais e da privacidade dos indivíduos – em especial

20. GILOVICH, Thomas; GRIFFIN, Dale; KAHNEMAN, Daniel. *Heuristics and biases: The psychology of intuitive judgment*. Cambridge University Press, 2002.

21. No original: "*Thus, they might not be willing to adopt a strict privacy protection strategy, since they doubt it will eventually pay-off*". (KOKOLAKIS, *op. cit.*, p. 5).

22. Daniel Kahneman, o psicólogo que ganhou o Nobel de Economia. Infomoney. Disponível: https://www.infomoney.com.br/perfil/daniel-kahneman/. Acesso: 09 jul. 2022.

considerando novas tecnologias, como é o caso dos *IoTs* –, sem se esquecer ou menosprezar o interesse do mercado atualmente configurado em torno das plataformas digitais.

Nesse sentido, é indispensável entender que os fatores que levaram a configuração desse fenômeno, e, para tanto, as razões aqui indicadas levam em consideração o estudo desenvolvido por Williams Meredydd, Jason Nurse e Sadie Creese[23].

No trabalho apresentado, uma das principais causas para o *privacy paradox* seria (i) a falta de experiência e familiaridade do usuário com temais ligados à área da tecnologia, uma vez que experimentos sociais feitos com os indivíduos[24] sugerem que aqueles com maior expertise no tema, tendem a ter configurações de privacidade mais rígidas. Neste ponto, pensando na relação desse fenômeno com os dispositivos *IoTs* – que será o próximo tópico deste estudo – tem-se que esse fator pode ser ainda mais relevante, tendo em vista que os usuários ainda possuem pouca familiaridade com tecnologias presente em nosso contexto desde o início da década de 90, quiçá com esses novos dispositivos, presentes e instrumentalizados de maneira muito diferente.

Outro fator apontado no estudo indicado, é (ii) o formato da usabilidade e o *design* das plataformas, isso porque, muitas delas são projetadas para que a coleta de dados seja feita. Nesse sentido, os autores ainda indicam *que "os indivíduos não tentam agir de forma insegura, mas a difícil usabilidade é um impedimento para que seu comportamento seja adequado"*[25]. Essa também é uma tendência em se tratando de dispositivos inteligentes, tendo em vista a ausência de uma interface direta do usuário com os mecanismos de privacidade dos *IoT* – já que a sua grande maioria funciona como "*plug and play*" – dificulta a possibilidade de ajuste da configuração padrão.

E dentro desse contexto, ainda que os usuários tenham interesse na modificação

23. WILLIAMS; NURSE; CREESE, 2018a, *op. cit.*, p. 02.

24. LEWIS, Kevin; KAUFMAN, Jason; CHRISTAKIS, Nicholas. *The taste for privacy: An analysis of college student privacy settings in an online social network.* Journal of Computer-Mediated Communication, vol. 14, 2008. Disponível em: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1083-6101.2008.01432.x. Acesso em: 10 jul. 2022.

25. No original: *"(…) individuals do not try to act insecurely, but poor usability is an impediment to correct behavior".* (WILLIAMS; NURSE; CREESE, 2018a, *op. cit.*, p. 03).

e alteração das regras de suas plataformas, estes encontram políticas de privacidade que, muitas vezes, estão escritas em uma linguagem de difícil compreensão. Por isso, ainda que os usuários tenham interesse no ajuste das configurações, estes tendem a ignorar as declarações dado os custos de transação em interpretar as regras ali descritas. Essa situação, por si só, configura o (iii) fator que leva a caracterização do *privacy paradox* – a qual também não parece ser modificada ao abordarmos os aspectos relacionados a tecnologia do *IoT*.

Também é indicado neste cenário a (iv) a falta de projeção dos riscos de privacidade pelo usuário, ou seja, a dificuldade em projetar no mundo virtual as medidas de segurança com a privacidade no mundo real. Isso porque "*enquanto todos sabem que trancar a porta impede a entrada não autorizada, as pessoas tendem a não entender as precauções equivalentes que podem tomar para proteger seus dados e dispositivos de comunicação no ciberespaço*" (tradução livre)[26].

Por fim, outro fator indicado pelos autores é (v) de que o contexto social dos usuários, os quais indicam as normas sociais que influenciam a conduta dos indivíduos, ou seja, as normas sociais ajudam a identificar o que seria considerado aceitável ou não. Isso significa que, a depender do contexto de cada indivíduo, a compreensão sobre o comportamento do usuário em relação aos seus dados pessoais pode variar, uma vez que o "aceitável" seria variável a depender de fatores culturais, de personalidade e idade, por exemplo.

Feita essa breve explicação os fatores que contribuem para a configuração do *privacy paradox*, passa-se a abordar a problemática principal deste artigo, com o objetivo de compreender como os dispositivos *IoT* podem se relacionar com essa discussão, e, em caso positivo, de que forma isso pode ocorrer.

26. No original: "*Whereas everybody knows that locking a door can prevent unauthorized entry, people tend not to understand the equivalent precautions they can take in order to protect their data and communications devices in cyberspace.*" (CREESE, Sadie; LAMBERTS, Koen. *Can cognitive science help us make information risk more tangible online?* Disponível em: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.335.3047&rep=rep1&type=pdf. Acesso em: 09 jul. 2022).

4. INTERNET DAS COISAS E *PRIVACY PARADOX*

Ao mencionar o termo "Internet das Coisas", quase que instantaneamente o relacionamos com os dispositivos que permitem aos usuários ligar ou desligar a televisão por um comando de voz ou, ainda, ativar a máquina de lavar por meio de um aplicativo em celular. Contudo, conforme conceituado por Rebecca Crootof, a mera conexão desses dispositivos por sensores e/ou *internet* não podem ser a razão pela qual estes não mais estariam classificados como "bobos", mas, "inteligentes"[27], se assim fosse, estaríamos tratando de automações, e não de IoT. Essa "inteligência", na verdade, decorre da sua capacidade *"de coletar e processar informações do ambiente ou das redes às quais estão conectadas"*[28], e isso altera radicalmente a tecnologia atual.

Considerando os dispositivos atuais, a maior parte deles é dependente de informações inseridas por indivíduos. Quase a totalidade das informações disponíveis na *internet* hoje, foram primeiramente capturadas e criadas por humanos, seja digitando, gravando, tirando fotos ou escaneando a informação[29]. Com os *IoTs*, a coleta de dados sobre as "coisas" é feita a qualquer momento e depender efetivamente de uma ação humana propriamente dita, gerando um volume de dados sem precedentes.

Essa tecnologia é revolucionária justamente por permitir que vários dispositivos conectem entre si, compartilhando e analisando dados do ambiente para entregar determinado serviço/produto. Por isso, o atual enfoque dos *IoTs* é criar ferramentas não muito caras e que se comuniquem entre si, com eficiência, para criar um ambiente melhor: um local no qual os objetos comuns possam agir com base no que precisamos e gostamos sem a necessidade de dar instruções e comandos expressos[30].

27. CROOTOF, Rebecca. *The Internet of Torts: expanding civil liability standards to address corporate remote interference*. Duke Law Journal. Durham: Duke University School of Law, v. 69, 2019, p. 586.
28. OLIVEIRA, Sérgio. *Internet das Coisas com ESP8266, Arduino e Raspberry PI*. São Paulo: Novatec, 2017, p. 15.
29. ASHTON, Kevin. *That 'Internet of Things' Thing*. RFID Journal. Alpharetta: Emerald X, jul. 2009.
30. RAYES, Ammar; SALAM, Samer. *Internet of Things – From Hype to Reality: The Road to Digitization*. New York: Springer, 2017, p. 1.

Neste ponto, se mostra imprescindível analisar as razões pelas quais os IoTs são considerados uma ruptura com a tecnologia atual. Assim, é preciso compreender as implicações deste novo cenário no que diz respeito a proteção de dados e privacidade, e, mais especificamente sobre o *privacy paradox*.

Apenas a título de contextualização sobre o tema, nesse mesmo estudo feito por Williams Meredydd, Jason Nurse e Sadie Creese[31] , que tinha como um dos objetivos identificar as razões que levam a compra de determinados produtos pelos usuários, revelou, entre muitas outras conclusões que (i) a privacidade raramente influenciava o critério de escolha dos usuários; e (ii) poucos indivíduos estavam familiarizados com os dispositivos *IoT*. Além disso, analisando os resultados qualitativamente, o estudo ainda demonstrou que alguns participantes ao serem questionados sobre a coleta de dados feitas por esses apetrechos responderam que *"são apenas configuração e coisas assim, nada para se preocupar"*[32], e, ainda, *"só porque são apenas atividades, é apenas o que eu faço, eu não vejo isso como um segredo"*[33], o que só ressalta a falta de familiaridade dos usuários com tal tecnologia.

As características aqui trabalhadas serão inspiradas em outro estudo, feitos por esses mesmos pesquisadores[34], esclarecendo-se ainda que estas não são exaustivas, tendo sido escolhidas para detalhamento aquelas consideradas mais relevantes para a abordagem do presente trabalho.

A primeira delas não poderia deixar de ser a ubiquidade dos dispositivos, dado que estes podem se estabelecer em todos os lugares, e, tendo em vista seu custo relativamente baixo, teríamos milhares de máquinas conectadas em rede, capazes de documentar e processar dados dos indivíduos como nunca feito antes[35]. Essa onipresença complexifica o debate, pois usuários comuns podem não ter ciência – ou

31. WILLIAMS; NURSE; CREESE, 2018a, op. cit., p. 01.
32. No original: (…) *"It's just settings and stuff like that, nothing to worry about"* (Ibid, p. 07).
33. No original: *(…) "Just because it's only activity, it's only what I get up to, I don't see it as a secret"* (Ibid, p. 07).
34. (WILLIAMS; NURSE; CREESE, 2018a, op. cit., p. 02).
35. HEROLD, Rebecca. *The Criticality of Security in the Internet of Things*. Isaca Journal, 2015. Disponível em: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2015/volume-6/the-criticality-of-security-in-the-internet-of-things_joa_eng_1115.pdf. Acesso em: 11 jul. 2022.

efetiva consciência – sobre eventual tratamento de dados feito por esses dispositivos no cotidiano que seriam de propriedade de terceiro. Seria inclusive um enigma entender em que momento o indivíduo é considerado "desconectado" da rede, já que mesmo desativando toda sua conexão, este ainda estaria ao arbítrio de todos os demais dispositivos atuando no serviço público ou simplesmente na casa de um conhecido.

Outra característica é a de que os apetrechos de *IoT* possuem pouca interface direta para com o usuário sobre o ajuste de suas configurações, alguns tem apenas alguns botões de comando e luzes indicativas de funcionamento. Por isso, ajustes na configuração padrão destes dispositivos dependem de aplicativos próprios ou acessos a sítios eletrônicos, friccionando a usabilidade destes itens. Parece relativamente "simples", mas, essa jornada – a qual muito possivelmente não é possível de ser adaptada tendo em vista o formato dos *IoTs* e sua aplicação – quando analisada sob o prisma da experiência do usuário, cria um desafio ainda maior e incentiva a inércia do usuário em atuar em favor da privacidade e proteção de seus dados pessoais[36], a qual será considerada uma dispendiosa.

O outro fator diz respeito a essa ser uma tecnologia nova, com a qual os indivíduos ainda não estão acostumados, tendo pouca familiaridade/experiência com seu funcionamento e configuração, o que cria um óbice para os usuários projetarem os eventuais riscos ligados ao uso de *IoTs*. E não é só: esses dispositivos são, inclusive, extremamente heterogêneos entre si, isso porque, possuem aplicação para uma infinidade de propósitos[37], como controle de produção industrial, automação de residências, empresas e até cidades (com as denominadas "*smart cities*"), e, claro, os dispositivos *wearables*, que seriam aqueles "usáveis" como os *smartwatches* e os recentes marcapassos. Por isso, considerando suas muitas vertentes de aplicação, e, seus diferentes formatos, é bem difícil para que o usuário tenha experiência prática com tais dispositivos.

36. SOUTHAMPTON. University of Southampton. *Making IoT configuration more secure and easy-to-use*. Disponível em: https://www.southampton.ac.uk/news/2015/09/iot-device-sensor-study.page. Acesso em: 10 jul. 2022.
37. CHRIST, Oliveir. *Martin Heidegger„s Notions of World and Technology in the Internet of Things age*. Asian Journal of Computer and Information Systems, v. 03, 2015.

Por fim, outro grande fator que influencia o debate entre *IoT* e a privacidade e proteção de dados é a influência do mercado na concepção do produto. Isso porque, a tendência atual é de que cada vez mais novas ferramentas e empresas participem do mercado competitivo de *IoT*, de forma que a sobrevivência desses *players* dependerá da redução de custos na fabricação desses dispositivos. Nestes casos, a contenção de despesas em geral não será aplicável para questões indispensáveis ao funcionamento e eficácia do produto, ao contrário, estas são aplicáveis em questões indiretas, como são as questões ligadas a segurança dos *IoTs*. Por isso, é relativamente possível imaginar que o incentivo do mercado de baixo custo sem a definição de requisitos e/ou garantias mínimas, poderá ocasionar a produção de dispositivos de baixo custo, em detrimento do uso de altos padrões de segurança: essa situação seria um possível evento de comprometimento da privacidade dos usuários em si, posto que deles não é esperado a conhecimento técnico para apurar essa informação tão complexa.

Apenas a título exemplificativo, alguns automóveis que fazem uso dessa tecnologia, por meio do sistema de chave denominado "*keyless*", tem sido alvo de ataques *hackers* por criminosos que se aproveitam da vulnerabilidade de segurança do dispositivo, dado o protocolo escolhido pela fabricante[38]. Conforme dados levantados pela empresa de segurança britânica Tracker, cerca de 92% (noventa e dois por cento) dos carros roubados e recuperados pela companhia em 2019 foram subtraídos sem utilizar a chave de seu proprietário[39].

Dito tudo isso, é importante ressaltar que ainda não temos um uso de *IoT* maduro e estável na sociedade, em especial quando consideramos a utilização doméstica destes dispositivos, ocasião em que os riscos a privacidade e proteção de dados dos usuários aqui indicados ainda parecem distantes e muitas vezes até factíveis de ocorrer. Contudo, conforme indicado no mencionado estudo, que serviu de base para a

38. REIS, Alessandro. *Furto de carro por hackers chega ao Brasil após virar epidemia na Europa*. Disponível em: https://www.uol.com.br/carros/noticias/redacao/2022/04/08/furto-de-carro-por-hackers-chega-ao-brasil-apos-explodir-na-europa.htm?cmpid=copiaecola. Acesso em: 09 jul. 2022.

39. THE RISE IN KEYLESS CAR THEFT. Tracker Network (UK) Limited. Disponível em: https://www.tracker.co.uk/tracker-hub/news/keyless-entry-systems-blamed-rise-car-theft-england-and-wales. Acesso em 09 jul. 2022.

análise desse trabalho *"uma vez que a IoT esteja firmemente estabelecida, os indivíduos começarão a considerar essas tecnologias como 'normais' e a abstenção pode ser considerada como antiquada"*[40] (tradução livre). E é justamente, por isso, que esse debate se mostra essencial.

5. MITIGAÇÃO DOS RISCOS E PROPOSTAS DE AJUSTE

Conforme descrito neste trabalho, foram apresentadas as várias formas pelas quais os dispositivos *IoT* podem influenciar e agravar a controvérsia decorrente do *privacy paradox,* em especial pelo fato de que essa nova tecnologia obstaculiza a autodeterminação informativa do usuário[41].

Várias discussões sobre o tema têm sido traçadas e muitas delas feitas mediante medidas propositivas, com soluções mitigadoras que podem equilibrar o direito à privacidade e proteção de dados dos usuários com o interesse das empresas – ou melhor dizendo, da ciência – sobre o uso dos *IoTs.* E, claro, não é demais lembrar neste ponto que, o objetivo deste trabalho não é levar a nenhum desestímulo ou crítica no uso de *IoT*, dado que, assim como qualquer dos demais serviços e produtos consumidos no dia a dia, são passíveis de apresentar riscos e potenciais vulnerabilidades. O principal ponto aqui é instigar o debate relacionado a privacidade, e analisar as atuais sugestões da doutrina para mitigar eventuais riscos e ofertar um produto melhor ao público.

Nesse sentido, a principal sugestão para reduzir essa disparidade está relacionada com o aumento da conscientização dos usuários. Uma pesquisa feita por Meredydd Williams, da Universidade de Oxford, a qual tinha como objetivo estudar a preocupação da privacidade dos usuários no uso de *smartwatches*, conduziu um experimento prático no qual os usuários foram informados de forma adequada sobre o

40. No original: *"once the IoT is firmly established individuals will begin considering these technologies as "normal" and abstention might be viewed as antiquated."*. 40 (WILLIAMS; NURSE; CREESE, 2018a, op. cit., p. 05).

41. Neste ponto, é importante destacar que o estudo feito pelos pesquisadores Williams Meredydd, Jason Nurse e Sadie Creese, chegou à conclusão, inclusive, de que os proprietários de dispositivos IoTs se importam menos com sua privacidade quando comparado com os demais. (WILLIAMS; NURSE; CREESE, 2018b, op. cit., p. 08).

tratamento de dados pessoais em tais dispositivos[42]. Conforme os resultados apontados, o nível de preocupação desses usuários aumentou razoavelmente depois da orientação feita e seu comportamento na rede passou a ser mais cuidadoso por semanas após essa interação – muitos dos usuários, por exemplo, realizaram ajustes de configurações no *smartwatch.* Estudos como esse, conseguem demonstrar e apontar com o uso de dados e experimentos empíricos que, com a abordagem correta, a conscientização dos usuários não seria uma proposta interventiva vazia ou sem resultados como muito se acredita.

Nessa mesma linha, e não menos importante, está a necessidade de adoção de declarações de privacidade das empresas de forma adequada, as quais devem ser transparentes e com o objetivo de buscar reduzir as disparidades e a assimetria informacional sobre o tratamento de dados pessoais naquela operação em específico[43]. Neste ponto, já é possível perceber que as empresas têm investido cada vez mais nessa comunicação mais assertiva e compatível com o perfil de seus usuários, trabalhando na divulgação de documentos com linguagem simples, acessível e fazendo uso de recursos visuais, que seria a técnica do *visual law* propriamente dito[44]. Apesar de no âmbito deste trabalho não ter sido encontrado nenhuma política com o uso de *legal design* nos dispositivos IoT, recomenda-se a leitura dos termos e condições de uso das empresas Koin e Will Bank, que são interativos, bem como do termo de abertura

42. WILLIAMS, Meredydd. *Exploring the inuence of privacy awareness on the Privacy Paradox on smartwatches*. University of Oxford: Thesis submitted for the degree of Doctor of Philosophy, 2018. Disponível em: https://ora.ox.ac.uk/objects/uuid:b4a1b178-34c8-49d2-bc80-0b4a23358959/download_file?file_format=pdf&safe_filename=thesis.pdf&type_of_work=Thesis. Acesso em: 09 jul. 2022.

43. ZIAR, Riaz Ahmand; OMAR, Rafiullah; SABER NIAZY, Irfan Ahmand. *Information Privacy Paradox and Fatigue in IoT* in Kardan Journal of Engineering and Technology, Kabul: Kardan Publications, 2019, p. 42. Disponível em: https://www.researchgate.net/profile/Irfan-Ahmad-13/publication/353321612_Information_Privacy_Paradox_and_Fatigue_in_IoT/links/60f3bdb516f9f313008ed65c/Information-Privacy-Paradox-and-Fatigue-in-IoT.pdf. Acesso em: 03 jul. 2022.

44. A propósito, a recomendação de documentos das empresas aplicáveis aos usuários como sendo feitos de forma mais acessível e simples, é inclusive recomendação da União Europeia em um estudo feito as atitudes dos consumidores frente os T&Cs. (COMISSÃO EUROPEIA, 2016, op. cit., p. 11)

de conta do Banco Inter, o qual utiliza de recursos visuais que facilita a compreensão dos usuários, sendo estes exemplos do bom uso da técnica aqui indicada.

Outra estratégia, é melhorar a forma de comunicação na interface dos dispositivos com o usuário, com o objetivo de evidenciar mais o risco de determinado *setup*[45]. Apesar de se assemelhar bastante com a outra medida indicada acima, neste caso o foco é a jornada do usuário com o IoT e sua jornada experiência de experiência ao ajustar as configurações aplicáveis. Neste caso, as empresas poderiam se valer de explicações descritivas as cada botão disponível para escolhas, grifos em partes importantes ou, simplesmente, exibir uma comunicação de aviso ao ativar determinadas configurações mais sensíveis.

Note que em qualquer das técnicas aqui indicadas, a ideia é de seguir as diretrizes mercadológicas ligadas ao "*customer centric*", no qual o usuário e seus interesses são colocados como ponto de partida para que as empresas possam desenvolver e/ou aprimorar soluções com base nesses anseios de seu consumidor.

É justamente por isso, que times de produto/técnicos, experiência do usuário e jurídico, devem trabalhar em conjunto para a implementação de tais recomendações para executar e colocar em prática os objetivos da empresa, sem se esquecer da necessidade de mitigar os riscos de assimetria informacional do usuário.

6. CONCLUSÃO

Diante do que se argumentou neste trabalho, é possível perceber que o conceito de privacidade sofreu drásticas alterações desde que esse foi inicialmente estabelecido, contudo, um entendimento que não foi modificado é o de que os indivíduos possuem certas preocupações de que o uso indiscriminado da tecnologia pode interferir em aspectos de sua vida privada.

No contexto atual, tem-se que grande parte dos usuários é relativamente preocupada com o tratamento ilegal de seus dados pessoais por terceiros, e menciona não compreender como justa a troca de informações privadas por melhores condições comerciais, por exemplo. Ao mesmo tempo, esses mesmos usuários estão na rede compartilhando fotos e vídeos, expressando suas opiniões nas redes sociais, além de

45. WILLIAMS; NURSE; CREESE, 2018a, *op. cit.*, p. 07.

usar produtos e serviços aceitando termos de uso e declarações de política de privacidade que sequer foram abertas, quanto mais lidas e/ou interpretadas. Em breve síntese, esse é o fenômeno do *privacy paradox,* diretamente ligado ao uso novas tecnologias, o qual tenta entender eventual dicotomia presente entre o comportamento "aparentemente" descuidado dos usuários com seus dados pessoais e a intenção e preocupação destes com sua privacidade e o tratamento ilegal e indevido de seus dados. Neste ponto, uma questão precisa ficar clara: a compreensão da fragilidade da posição do usuário nessa relação e os vieses comportamentais que resultam nesse *privacy behaviour* que é compreendido, muitas vezes, como "negligente", quando, na verdade, outras razões podem ser aplicáveis, conforme indicado neste trabalho.

Em outro aspecto, analisou-se a tecnologia *IoT* e porque essa é considerada tão inovadora e diferente de tudo que já se tinha expertise nos tempos atuais. Nesse sentido, foram explicadas que as características inerentes a tais dispositivos e de que forma estas poderiam implicar em riscos pela privacidade, até então, pouco conhecidos: como o fato de os *IoTs* poderem estar em todo lugar e a qualquer tempo, tornando complexo para o usuário compreender se ele está ou não em um ambiente monitorado e, se sim, quais seriam os seus dados ali coletados? Sob o domínio de qual empresa estariam suas informações? Além disso, a falta de influência do mercado – e aqui se fala de setor público e privado – sobre a necessidade de se exigir padrões mínimos de segurança a esses dispositivos ofertados ao público. Ou, ainda, a coleta de dados e informações em quantidade e velocidade de processamento sem precedentes, tornando difícil imaginar quais seriam todas as implicações relacionadas ao uso de *IoTs*.

Por outro lado, fato é que ainda não atingimos a maturidade no uso desses dispositivos na sociedade, seu uso ainda é extremamente recente, tornando o momento atual ideal para discutirmos eventuais medidas mitigadoras que poderiam ser adotadas para uso dessa nova tecnologias. Por exemplo, a exigência de determinados padrões de usabilidade e interface com o usuário ao utilizar esses dispositivos e, ainda, o aumento do nível de informação do usuário sobre seu real funcionamento.

Neste aspecto, o objetivo deste trabalho promover as discussões necessárias ao uso dos *IoTs* no que diz respeito aos atuais riscos de privacidade e proteção de dados, já mapeados até aqui, uma vez que não há dúvidas sobre a importância e imprescindibilidade desses dispositivos na sociedade atual.

REFERÊNCIAS

ACQUISTI, Alessandro. *Privacy in electronic commerce and the economics of immediate gratification*, 2004. Disponível em: https://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf. Acesso em: 09 jul. 2022

ALEMANHA. *High Court of Dusseldorf. Caso V1-Kart 1/19*, 26 de agosto de 2019, p. 25. Disponível em: https://www.d-kart.de/wp-content/uploads/2019/08/OLGD%C3%BCsseldorf-Facebook-2019-English.pdf. Acesso em: 04 jul. 2022

ASHTON, Kevin. *That 'Internet of Things' Thing*. RFID Journal. Alpharetta: Emerald X, jul. 2009.

CARRASCAL, Juan Pablo; RIEDERER, Christopher; ERRAMILLI, Vijay; e CHERUBINI, Mauro. *Your browsing behavior for a big mac: Economics of personal information online*, in 22nd International Conference on World Wide Web, 2013, pp. 189–200.

CHRIST, Oliveir. *Martin Heideggers Notions of World and Technology in the Internet of Things age*. Asian Journal of Computer and Information Systems, v. 03, 2015. 58–64.

COMISSÃO EUROPEIA. Comissão Europeia. Study on consumers' attitudes towards Terms and Conditions (T&Cs), 2016, p. 11. Disponível em: https://ec.europa.eu/info/sites/default/files/terms_and_conditions_final_report_en.pdf. Acesso em: 05 jul 2022.

CREESE, Sadie; LAMBERTS, Koen. *Can cognitive science help us make information risk more tangible online?* Disponível em: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.335.3047&rep=rep1&type=pdf. Acesso em: 09 jul. 2022

CROOTOF, Rebecca. *The Internet of Torts: expanding civil liability standards to address corporate remote interference*. Duke Law Journal. Durham: Duke University School of Law, v. 69, n. 03, p. 583-667, 2019.

DANIEL KAHNEMAN, O PSICÓLOGO QUE GANHOU O NOBEL DE ECONOMIA. Infomoney. Disponível: https://www.infomoney.com.br/perfil/daniel-kahneman/. Acesso: 09 jul. 2022.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 117.

GILOVICH, Thomas; GRIFFIN, Dale; KAHNEMAN, Daniel. *Heuristics and biases: The psychology of intuitive judgment*. Cambridge University Press, 2002.

HEROLD, Rebecca. *The Criticality of Security in the Internet of Things*. Isaca Journal, 2015. Disponível em: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2015/volume-6/the-criticality-of-security-in-the-internet-of-things_joa_eng_1115.pdf. Acesso em: 11 jul. 2022.

https://mjrobot.org/2017/01/06/o-iot-feito-simples-monitorando-a-temperatura-desde-qualquer-lugar/. Acesso em: 08 jul. 2022.

IOT NA MEDICINA: COMO FUNCIONA E EXEMPLOS. Folha Tecno. Disponível em:

https://www.folhatecno.com.br/2021/10/iot-medicina-como-funciona.html. Acesso em: 05 jul. 2022.

KOKOLAKIS, Spyros. *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*. Dept. of Information & Communication Systems Engineering, University of the Aegean, 2015, p. 4. Disponível em: https://www.researchgate.net/publication/280244291. Acesso em: 08 jul. 2022.

LEWIS, Kevin; KAUFMAN, Jason; CHRISTAKIS, Nicholas. *The taste for privacy: An analysis of college student privacy settings in an online social network*. Journal of Computer-Mediated Communication, vol. 14, 2008, p. 79– 100. Disponível em: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1083-6101.2008.01432.x. Acesso em: 10 jul. 2022.

MONTEIRO, Gabriela Reis Paiva. *Big data e concorrência: uma avaliação dos impactos da exploração do big data para o método antitruste tradicional de análise das concentrações econômicas*, 2017. Dissertação (Mestrado em Direito) – Escola de Direito Getúlio Vargas, Rio de Janeiro.

MREDYDD, Williams; NURSE, Jason; CREESE, Nurse. "*Privacy is the Boring Bit": User Perceptions and Behaviour in the Internet-of-Things*. Department of Computer Science, University of Oxford, 2018b, p. 01.

OLIVEIRA, Sérgio. *Internet das Coisas com ESP8266, Arduino e Raspberry PI.* São Paulo: Novatec, 2017.

PARENTONI, Leonardo. O Direito ao Esquecimento (Right to Oblivion). In: DE LUCCA, Newton et al. Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015, p. 539-618.

RAYES, Ammar; SALAM, Samer. *Internet of Things – From Hype to Reality: The Road to Digitization*. New York: Springer, 2017.

REIS, Alessandro. *Furto de carro por hackers chega ao Brasil após virar epidemia na Europa.* Disponível em: https://www.uol.com.br/carros/noticias/redacao/2022/04/08/furto-de-carro-por-hackers-chega-ao-brasil-apos-explodir-na-europa.htm?cmpid=copiaecola. Acesso em: 09 jul. 2022.

ROVAI, Marcelo. *O IoT feito simples: Monitorando a temperatura desde qualquer lugar.* Disponível em:

https://mjrobot.org/2017/01/06/o-iot-feito-simples-monitorando-a-temperatura-desde-qualquer-lugar/. Acesso em: 08 jul. 2022.

SOUTHAMPTON. University of Southampton. *Making IoT configuration more secure and easy-to-use.* Disponível em: https://www.southampton.ac.uk/news/2015/09/iot-device-sensor-study.page. Acesso em: 10 jul. 2022.

SPIEKERMANN, Sarah; GROSSKLAGS, Jens; BERENDT, Bettina. *E-privacy in 2nd Generation ECommerce: Privacy Preferences versus actual Behavior*, 2001. Disponível em: https://www.researchgate.net/publication/2480871_E-privacy_in_2nd_Generation_E-

Commerce_Privacy_Preferences_Versus_actual_Behavior. Acesso em: 08 jul. 2022.

THE RISE IN KEYLESS CAR THEFT. Tracker Network (UK) Limited. Disponível em: https://www.tracker.co.uk/tracker-hub/news/keyless-entry-systems-blamed-rise-car-theft-england-and-wales. Acesso em 09 jul. 2022.

TUROW, Joseph; HENNESSY, Michael; DRAPER, Nora. *The Tradeoff Fallacy - How Marketers Are Misrepresenting esenting American Consumers and Opening Them up to Exploitation*. University of Pennsyvania, 2015, p. 3-4. Disponível em: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1554&hx0026;context=asc_papers. Acesso em: 05 jul. 2022.

WARREN, Samuel; BRANDEIS, Louis. *The Right to Privacy*. Harvard Law Review. Cambridge. Harvard University Press. v. IV, n. 05, p. 193-217, Dec. 1890. p. 194.

WILLIAMS, Meredydd. *Exploring the inuence of privacy awareness on the Privacy Paradox on smartwatches.* University of Oxford: Thesis submitted for the degree of Doctor of Philosophy, 2018. Disponível em: https://ora.ox.ac.uk/objects/uuid:b4a1b178-34c8-49d2-bc800b4a23358959/download_file?file_format=pdf&safe_filename=thesis.pdf&type_of_work=Thesis. Acesso em: 09 jul. 2022.

WILLIAMS, Meredydd; NURSE, Jason; CREESE, Sadie. *The Perfect Storm: The Privacy Paradox and the Internet-of-Things*. University of Oxford, 2018a, p. 01. Disponível em: https://ieeexplore.ieee.org/abstract/document/7784629#citations. Acesso em: 03 jul. 2022.

ZIAR, Riaz Ahmand; OMAR, Rafiullah; SABER NIAZY, Irfan Ahmand. *Information Privacy Paradox and Fatigue in IoT* in Kardan Journal of Engineering and Technology, Kabul: Kardan Publications, 2019, p. 42. Disponível em: https://www.researchgate.net/profile/Irfan-Ahmad-13/publication/353321612_Information_Privacy_Paradox_and_Fatigue_in_IoT/links/60f3bdb516f9f313008ed65c/Information-Privacy-Paradox-and-Fatigue-in-IoT.pdf. Acesso em: 03 jul. 2022.

IV
INTERNET DAS COISAS E CIBERSEGURANÇA

CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO APLICADAS À IOT

Victor Takashi Hayashi
Mestre em Engenharia da Computação pela Escola Politécnica da USP.

DOI: https://doi.org/10.59224/dti5.ch12

Resumo: O objetivo deste capítulo é apresentar conceitos de segurança da informação e cibersegurança no contexto de Internet das Coisas (IoT). Após a leitura deste texto, é esperado que o leitor tenha condições de analisar a segurança de sistemas IoT a partir da compreensão das demandas de segurança (requisitos), pontos fracos existentes (vulnerabilidades), motivações dos atacantes, e possíveis estratégias a serem adotadas para elevar o nível de segurança (prevenção e detecção). O artigo também conta com estudos de caso e algumas recomendações sobre como lidar com novos desafios de segurança em IoT.

Palavras-chave: Cibersegurançaç Internet das Coisasç Segurança da Informação.

Abstract: *The objective of this chapter is to present concepts of information security and cybersecurity in the context of the Internet of Things (IoT). Upon reading, it is expected that the reader will be able to analyze the security of IoT systems from the understanding of security demands (requirements), existing weaknesses (vulnerabilities), motivations of attackers, and possible strategies to be adopted to raise the level of security (prevention and detection). The article also features case studies and some recommendations on how to deal with new security challenges in IoT.*

Keywords: *Cybersecurity; Internet of Things; Information Security.*

1. O QUE É SEGURANÇA DA INFORMAÇÃO?

Quando os sistemas computacionais atuavam majoritariamente no mundo virtual, a segurança da informação surgiu como uma área do conhecimento que busca

entender as ameaças e ataques possíveis aos sistemas e atuar para diminuir o risco associado a estes ataques, implementando contramedidas efetivas.

Convém destacar que o nome em português *segurança da informação* remete a tornar seguro a manipulação de informações sensíveis e privadas que os usuários fornecem aos sistemas computacionais.

Por exemplo: quando um usuário fornece suas informações pessoais a alguma plataforma *online*, ele confia que a guarda destas informações será feita pela empresa responsável pela plataforma, que deve entender os ataques mais relevantes e atuar proativamente para mitigar seus possíveis efeitos negativos.

Ao pensar em segurança da informação, podemos lembrar apenas do uso de mecanismos de criptografia para prevenir ataques cibernéticos. De fato, a criptografia é um dos mecanismos de segurança mais utilizados, porém não é o único.

Considerar a segurança da informação apenas como aplicar criptografia para mitigar ataques às informações presentes no mundo virtual é uma visão limitada e que pode restringir as discussões sobre impactos dos ataques realizados em sistemas de Internet das Coisas (IoT) e as possíveis contramedidas, que inclusive abordam não só a prevenção aos ataques, mas também a detecção e recuperação a estes ataques de forma automática.

2. O QUE É CIBERSEGURANÇA?

O termo Cibersegurança remete ao termo em inglês *Cybersecurity*, que é a segurança do mundo virtual. Pode parecer em primeiro momento que as definições de segurança da informação e Cibersegurança se confundem de tal forma que não seria possível distingui-las. Porém, há uma linha tênue, porém, existente entre estes dois conceitos.

Se o termo segurança da informação diz respeito à guarda das informações fornecidas pelos usuários, podemos considerar que estas informações residem no mundo virtual, e que é necessário mitigar possíveis ataques que podem expor estas informações sensíveis a agentes não autorizados em eventos que conhecemos na mídia como *data breach*.

Por outro lado, podemos considerar que a Cibersegurança está relacionada com

a segurança no mundo virtual, abrangendo todos os possíveis ataques que ocorrem neste mundo virtual. Ou seja, podemos pensar que a Cibersegurança é mais abrangente que a segurança da informação, considerando sua semântica em português.

E o que isso tem a ver com Internet das Coisas? Acontece que sistemas IoT não só operam no mundo virtual, mas também no mundo físico. Se o IoT é uma tecnologia emergente que integra os mundos físico e virtual ao fornecer aos computadores a capacidade de sentir o mundo físico de forma autônoma[1], os impactos de seus ataques também não se limitam ao mundo virtual.

É possível que ataques ocorridos no mundo virtual tenham consequências imediatas no mundo físico, como o controle de um chuveiro inteligente em ima casa conectada por um atacante causar queimaduras em um ser humano. Ao tratar Cibersegurança como a área de conhecimento relacionada aos ataques ocorridos no mundo virtual, podemos abranger o exemplo de ataque descrito no ambiente de casa conectada.

Porém, ao tratar do termo segurança da informação, podemos dar a entender que estamos preocupados apenas com ataques que prejudicam a guarda segura das informações sensíveis dos usuários, o que pode restringir nossa visão sobre ataques, impactos e contramedidas.

3. O QUE DEMANDAR DE SEGURANÇA?

O primeiro passo para entender Cibersegurança e segurança da informação de um sistema é compreender o que demandamos de nível de segurança deste sistema.

Não há sistema 100% seguro. Sempre haverá algum ponto fraco (que definiremos a seguir como vulnerabilidades) que pode ser explorada, seja porque houve uso errado de mecanismos de segurança na implementação do sistema, ou até pelo fator humano (mal uso do sistema). É impossível ter um sistema 100% seguro, mas podemos almejar obter um sistema cada vez mais seguro, de forma que a segurança passa a ser um aspecto de qualidade deste sistema. E claro, como qualquer aspecto de qualidade, custa caro manter um nível alto de segurança.

Além de estar associada a um nível, a segurança de um sistema está associada a

1. ASHTON, Kevin et al. *That 'internet of things' thing.* RFID journal, v. 22, n. 7, p. 97-114, 2009.

requisitos específicos como não repúdio, confidencialidade, integridade, autenticidade e disponibilidade. Para nossa discussão, vamos salientar os requisitos Confidencialidade, Integridade e Disponibilidade, que em inglês formam a tríade CIA (*Confidentiality, Integrity, Availability*)[2].

A confidencialidade está associada com a definição de segurança da informação apresentada anteriormente. Quando usuários fornecem informações pessoais a algum sistema, um aspecto relevante da guarda destas informações é manter as informações confidenciais. Isto é, as informações devem ser confidenciais apenas aos agentes que possuem autorização para acessar esta informação.

Considere um exemplo de um sistema de apoio a um hospital, conforme ilustrado pela Figura 1. Ao fornecer endereço, idade, resultados de exames e outros, a ideia é que estas informações sejam confidenciais aos agentes autorizados: o próprio paciente e a equipe médica por exemplo. O hospital deve tanto impedir que terceiros não autorizados obtenham estas informações por meio de um ataque ao sistema de apoio, quanto garantir por meio de políticas internas que seu agente autorizado não irá fazer mal uso das informações confidenciais dos pacientes (para abrir uma conta no banco e obter um empréstimo, por exemplo).

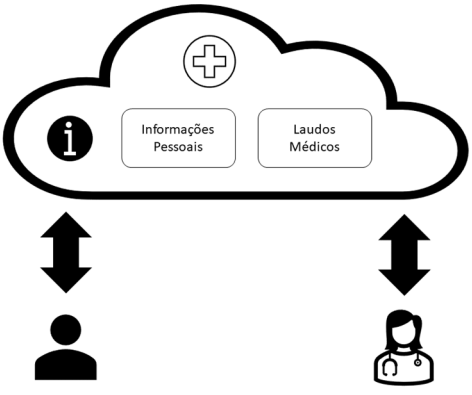


Figura 1 – Sistema de Apoio para Hospital. Fonte: Autoria Própria.

O segundo requisito importante para discussão é a Integridade. Além de impedir que a informação pessoal de usuários seja mantida confidencial, o responsável pelo

2. HINTZBERGEN, Jule et al. *Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002*. Brasport, 2018.

sistema computacional também deve garantir que esta informação não foi alterada de forma não autorizada. Ou seja, a informação deve estar íntegra. Ainda no exemplo de sistema de apoio a um hospital, caso algum atacante consiga forjar laudos médicos no sistema, ele pode enganar algum empregador com o laudo fraudado e levar à contratação de alguma pessoa que não tem condições físicas de exercer uma função específica. Desta forma, garantir que a informação do laudo não foi alterada e está da mesma forma que o médico legítimo forneceu ao sistema. Outro exemplo neste cenário, ainda mais preocupante, é fraudar laudos de exames de corpo de delito ou do Instituto Médico Legal (IML).

Por fim, temos o requisito de Disponibilidade. A definição formal diz que é o nível em que o sistema está disponível para uso pelo usuário autorizado no momento de sua tentativa de uso. Sistemas críticos tendem a demandar um alto nível de disponibilidade, de forma que falhas e ataques a estes sistemas causam eventos de indisponibilidade de forma muito rara, devido aos mecanismos de segurança e de tolerância a falhas adotados. Vamos voltar novamente ao exemplo do hospital, e considerar que o sistema de apoio também contempla serviços de atendimento para sanar dúvidas e obter informações sobre procedimentos de agendamentos e inclusive como proceder em casos de emergência. Se algum ataque levar à indisponibilidade deste sistema, então em eventos de alguma catástrofe ou mal súbito o sistema pode estar indisponível para os usuários legítimos, o que pode causar demora no atendimento e eventuais danos às pessoas.

4. VULNERABILIDADES DE UM SISTEMA

Após compreender alguns requisitos de segurança para deixar claro o que devemos demandar de segurança de um sistema de forma específica para fomentar discussões mais objetivas, vamos apresentar o conceito de vulnerabilidades, e relacionar este conceito com sistemas IoT.

As vulnerabilidades de um sistema são seus pontos fracos, que podem ser explorados por atacantes e se tornarem ameaças à segurança destes sistemas. Pode-se dizer que a existência de vulnerabilidades é essencial para que os ataques sejam realizados com sucesso e prejudiquem a confidencialidade e integridade de informações de usuários, e a disponibilidade de sistemas.

A verdade é que atacantes não buscam atacar os pontos fortes de um sistema, e sim seus pontos fracos para economizar tempo e recursos. A ideia é que, se há uma forma mais fácil e com menor custo para se realizar um ataque, então o atacante irá optar pelo caminho mais fácil e com maiores chances de sucesso.

Considere o exemplo de um ataque de força bruta na conta de algum usuário em específico de uma plataforma em nuvem. Neste tipo de ataque, há tentativas de se obter uma senha ao tentar diversas combinações possíveis. Se a plataforma tiver a vulnerabilidade de permitir tentativas incorretas consecutivas em um curto intervalo, então este ataque é possível. Por outro lado, se uma plataforma que estava sofrendo com este tipo de ataque utilizar algum mecanismo de bloqueio após algumas tentativas incorreras, então o atacante pode tentar explorar algum outro ponto fraco do sistema.

É possível simplificar o funcionamento de um sistema IoT considerando que ele é composto por dispositivos que possuem sensores e atuadores e serviços em uma plataforma de computação em nuvem, conforme pode ser observado na Figura 2. Os dispositivos possuem conexão com a Internet e conseguem sentir o mundo físico por meio de seus sensores, enviar estes dados para a plataforma em nuvem, além de obter informações e comandos desta mesma plataforma para modificar o mundo físico por meio de seus atuadores. Os usuários interagem com os dispositivos que possuem sensores e atuadores diretamente, ou então por meio de interfaces de usuário em celulares e computadores[3].

3. DE MORAES, Alexandre; HAYASHI, Victor Takashi. *Segurança em IoT: Entendendo os riscos e ameaças em IoT*. Rio de Janeiro: Alta Books, 2021.

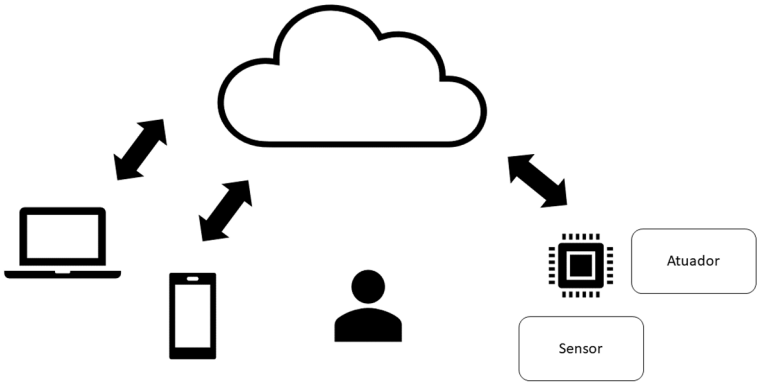


Figura 2 – Modelo Simples de um Sistema IoT. Fonte: Autoria Própria.

O desafio de segurança em sistemas IoT está associado à presença de vulnerabilidades em todos estes componentes. Por exemplo, uso de credenciais fixas ou senhas padrão para acesso aos dispositivos são vulnerabilidades relevantes[4]. A falta de mecanismos de criptografia em dispositivos IoT devido às suas restrições de consumo de energia, banda de comunicação, armazenamento e processamento limitados também é outra vulnerabilidade[5]. Mecanismos falhos de controle de acesso e autenticação em plataformas em nuvem também tornam possível a execução de ataques em escala afetando muitos dispositivos de uma só vez. A lista de vulnerabilidades continua e não é exaustiva, mas o que é importante é considerar que para cada caso é relevante levantar os pontos fracos existentes em um sistema IoT, pois estas vulnerabilidades que podem ser exploradas e são estes pontos fracos que tornam os ataques possíveis.

5. MOTIVAÇÕES DOS ATACANTES

Além da oportunidade fornecida pelas vulnerabilidades de um sistema IoT, para que algum ataque aconteça é necessário que exista alguma motivação para a execução

4. MIESSLER, Daniel. *Securing the internet of things: Mapping attack surface areas using the OWASP IoT top 10*. In: RSA conference. 2015.
5. DE MORAES, Alexandre; HAYASHI, Victor Takashi. *Segurança em IoT: Entendendo os riscos e ameaças em IoT*. Rio de Janeiro: Alta Books, 2021.

do ataque. Realizar ataques custa tempo e recursos. Por exemplo, para realizar um ataque de força bruta para obter uma senha, parte do processamento de um ou mais computadores é utilizada para tentar as diferentes combinações possíveis.

Pense em quanto tempo de processamento seria necessário para palpitar diferentes combinações de senhas de 4 dígitos numéricos. Talvez não demore tanto, mas se a senha tiver caracteres alfanuméricos e um tamanho bem maior, pode demandar muito mais tempo de processamento, ou seja, o ataque custa mais recursos.

Por isso, para entender como os ataques cibernéticos ocorrem, além da análise de vulnerabilidades citada anteriormente, é importante compreender as motivações dos atacantes. Nos exemplos anteriores, podemos levantar algumas hipóteses das razões para a motivação dos atacantes. O ataque de obter dados pessoais de pacientes para abrir uma conta bancária sem autorização pode ter uma motivação de ganho financeiro. Forjar laudos médicos também poderia alimentar algum esquema de fraude maior com ganho monetário. Ataques que tornam algum serviço essencial indisponível, como uma negação de serviço do telefone de emergência de uma cidade pode ter motivação ideológica ou apenas a satisfação em causar caos.

De qualquer forma, é importante levantar as motivações de atacantes e caracterizar estes agentes tanto para entender seu modo de operação, quanto eventualmente antecipar seu comportamento após a adoção de mecanismos de segurança, para se precaver sobre a próxima vulnerabilidade a ser explorada por estes atacantes.

6. ESTRATÉGIAS DE SEGURANÇA

Após entender os requisitos de segurança, as vulnerabilidades e as motivações dos atacantes, podemos identificar alguns ataques possíveis no sistema IoT.

Considere um exemplo de uma cidade inteligente cujo tráfego de veículos e pedestres é controlado por um sistema central que a partir de câmeras identifica a quantidade de veículos e pedestres nas vias e toma as melhores decisões de temporização para os semáforos da cidade, conforme ilustrado na Figura 3. Além da disponibilidade do sistema, outro requisito relevante é a integridade dos comandos.

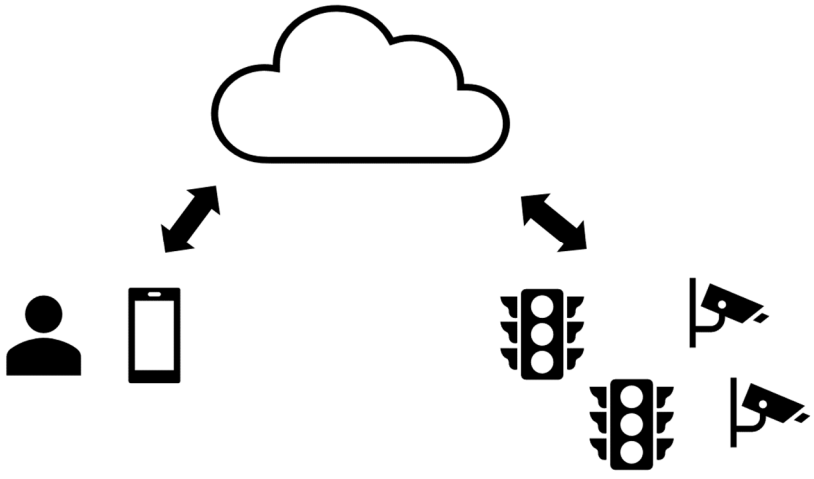


Figura 3 – Cidade Inteligente com Controle de Tráfego. Fonte: Autoria Própria.

Vamos considerar que o sistema possui dias vulnerabilidades: algoritmo de criptografia fraco para o envio de comandos do sistema central para os semáforos, e ter o sistema central como uma entidade central, um ponto único de falha que concentra toda a inteligência das tomadas de decisão quanto ao tráfego da cidade.

Um atacante que está insatisfeito com o sistema de tráfego pois em uma ocasião o levou a chegar atrasado em seu trabalho e ser demitido pode ter conhecimentos sobre o sistema pois auxiliou na sua implantação, e pode primeiro utilizar suas credenciais antigas para obter acesso interno ao sistema e realizar comandos manuais que levem a um congestionamento enorme na cidade.

Outra possibilidade é o atacante realizar o ataque de forma externa ao sistema, ao interceptar mensagens enviadas pela comunicação sem fio, decifrá-las devido ao uso de algoritmos fracos de criptografia, modificá-los e causar o congestionamento.

Por fim, é possível que o atacante utilize máquinas infectadas por um vírus para efetuar um ataque massivo ao sistema de tráfego centralizado. Com uma demanda gigante de requisições, o servidor pode exaurir seus recursos e se tornar indisponível. Como é um ponto único de falha, todo o controle de tráfego pode se tornar indisponível, levando ao congestionamento.

São formas diferentes de se chegar ao mesmo resultado do ataque, e o atacante pode optar por uma alternativa em específico de acordo com sua familiaridade com

o tipo de ataque, recursos necessários e vulnerabilidades presentes.

Para mitigar estes ataques, podemos tanto atuar na prevenção quanto na detecção e recuperação dos ataques. Como ataques em sistemas IoT são complexos e a adoção de medidas de segurança tradicionais pode não ser adequado devido às restrições dos dispositivos IoT, empregar técnicas e mecanismos variados pode ser a chave para aumentar o nível de segurança destes sistemas[6].

7. MECANISMOS DE PREVENÇÃO

Se quando pensamos em segurança da informação restringimos nossa visão aos algoritmos de criptografia, o mesmo ocorre com maior frequência quando pensamos em mecanismos para prevenir ataques. O uso de criptografia é uma das formas de se evitar ataques, atuando mesmo antes de sua ocorrência, porém há outros mecanismos essenciais como a Autenticação e o Controle de Acesso.

A autenticação é uma das primeiras barreiras contra atacantes. Para diferenciar usuários legítimos de atacantes, o processo de autenticação busca verificar se alguém é quem diz ser[7].

A forma mais utilizada para verificar a identidade de alguém é se apoiar em algum segredo, que é chamado de senha. Ao fornecer um usuário e uma senha para um sistema computacional, o usuário está comprovando que sabe de um segredo que somente ele deveria saber. Há formas de se autenticar com um dispositivo confiável (vide o uso de tokens por instituições bancárias), além de também existir uma adoção cada vez maior de autenticação baseada em características físicas únicas de cada indivíduo, como sua digital, face ou palma da mão.

Um desafio adicional em sistemas IoT é que há necessidade de se autenticar dispositivos também, o que pode ser realizado por meio de segredo ou certificados digitais (este último demanda um maior uso de recursos computacionais). Da mesma

6. DE MORAES, Alexandre; HAYASHI, Victor Takashi. *Segurança em IoT: Entendendo os riscos e ameaças em IoT*. Rio de Janeiro: Alta Books, 2021.
7. HAYASHI, Victor Takashi. *Non-invasive authentication for hands-free financial transactions in trusted connected locations*. 2022. Dissertação (Mestrado em Sistemas Digitais) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2022. doi:10.11606/D.3.2022.tde-21062022-140511.

forma que não desejamos ser enganados e permitir o acesso a atacantes que fingem ser usuários legítimos, também não desejamos nos comunicar com dispositivos que fingem ser dispositivos legítimos, e que na verdade tentam obter informações confidenciais de forma não autorizada.

Outro mecanismo é a famosa criptografia. Os algoritmos de criptografia buscam trabalhar em textos originais, que também são chamados de textos às claras, onde a informação pode ser visualizada por qualquer um, e transformá-los em textos cifrados, que são textos embaralhados que não permitem aos atacantes obter a informação original se não tiverem chaves específicas. Estas chaves estão em poder dos usuários legítimos, que podem embaralhar e desembaralhar (criptografar e decriptografar) as mensagens de forma a garantir sua confidencialidade e integridade.

Em sistemas IoT, podemos empregar métodos de criptografia com menor custo computacional (*lightweight cryptography*) para manter as medidas de sensores e comandos de atuadores íntegros e confidenciais. Porém, como os dispositivos possuem limitações de uso de banda de comunicação, energia restrita (se a fonte de energia for uma bateria), além de capacidades de processamento e armazenamento menores que os computadores convencionais de última geração. Desta forma, ainda são empregados esforços para permitir o uso de criptografia em sistemas IoT, dado que não é possível empregar diretamente os mesmos mecanismos de criptografia tradicionais devido às limitações dos dispositivos IoT, pois estes mecanismos usuais seriam muito onerosos[8].

Por fim, há também o controle de acesso, que contempla tanto a gestão efetiva de credenciais quanto um controle de acesso a arquivos e ambientes de forma a limitar os danos causados pelo comprometimento de credenciais. No exemplo anterior de ataque a uma cidade inteligente, uma vulnerabilidade explorada foi a manutenção da credencial de um funcionário demitido com acesso pleno ao sistema de controle de tráfego. Uma gestão efetiva de credenciais busca evitar situações como essa, de forma a suportar o ciclo de vida de credenciais, desde a criação de credenciais até sua exclusão ou inativação.

Por outro lado, fornecer um acesso limitado somente aos arquivos e ambientes

8. DE MORAES, Alexandre; HAYASHI, Victor Takashi. *Segurança em IoT: Entendendo os riscos e ameaças em IoT*. Rio de Janeiro: Alta Books, 2021.

que cada usuário deve ter acesso para executar suas funções pode limitar o impacto de ataques de engenharia social. Imagine que o atacante tente persuadir um funcionário de uma empresa terceirizada que trabalha com registros de manutenções realizadas no sistema de controle de tráfego da cidade inteligente. Se obter as credenciais deste funcionário com sucesso, a ideia é que ele só tenha um acesso restrito para as funcionalidades de registro de manutenção, e não deve ter acesso aos comandos enviados aos semáforos inteligentes.

8. MECANISMOS DE DETECÇÃO

Além dos mecanismos de prevenção, é importante destacar que também é possível atuar na detecção e recuperação de ataques. Como os atacantes estão cada vez mais sofisticados e os ataques mais complexos, pode ser muito difícil prevenir com sucesso que atacantes tenham acesso ao sistema computacional. Porém, mesmo que estes atacantes tenham entrado no ambiente, é possível empregar mecanismos que agem em tempo real, durante a execução do ataque para limitar seu impacto e retirar o invasor do ambiente.

Neste sentido, sistemas de detecção de intrusão são muito similares em funcionamento ao sistema biológico humano. Ao encontrar comportamentos suspeitos, os agentes de defesa buscam agir no sentido de proteger o corpo humano a partir de diversas estratégias. No contexto de Internet das Coisas, é necessário entender o comportamento de usuários e dispositivos. Como muitos destes sistemas empregam dezenas de dispositivos e usuários, e milhares de pacotes de dados por dia, é necessário ter meios automatizados para identificar comportamentos suspeitos e atuar de forma ágil. Esta é uma ótima oportunidade para algoritmos inteligentes de Inteligência Artificial conseguirem aprender estes padrões de intrusão e auxiliarem a aumentar o nível de segurança de sistemas IoT[9].

9. CRUZ, Antonia Raiane Santos Araujo; GOMES, Rafael Lopes; FERNANDEZ, Marcial Porto. *DIMI: Detecção Inteligente de Botnets Mirai em Redes IoT*. Anais do Computer on the Beach, v. 12, p. 362-369, 2021.

9. ESTUDO DE CASO

Para demonstrar como os conceitos apresentados podem ser úteis para a análise de segurança de sistemas IoT, será apresentado um estudos de caso de ataque real. O *framework* de avaliação irá levar em conta os seguintes aspectos:

- Quais requisitos de segurança são impactados (Confidencialidade e Integridade das informações, ou Disponibilidade do sistema);
- Quais vulnerabilidades foram exploradas;
- Quais as possíveis motivações dos atacantes;
- Quais estratégias e mecanismos de segurança poderiam ser empregados.

O Botnet Mirai é o estudo de caso ilustrado na Figura 4.

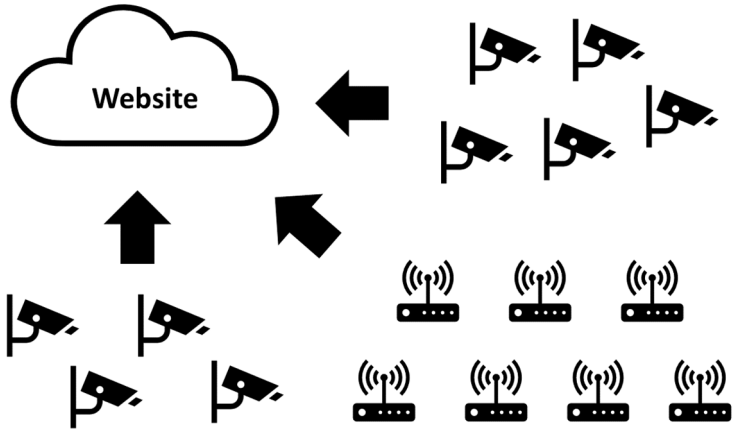


Figura 4 – Ataque Botnet Mirai. Fonte: Autoria Própria.

Para entender o ataque, vamos apresentar uma breve descrição, conforme descrito por Prado[10]:

"*Entre agosto e outubro de 2016, o malware Mirai, utilizando uma larga escala de botnets IoT, foi responsável por alguns dos maiores ataques DDoS já registrados (...) deixando centenas de websites fora do ar - incluindo Twitter, Netflix, Reddit, e*

10. PRADO, Marcelo Alves. *Análise experimental da botnet IoT Mirai*. 2018. 68 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de informação) - Universidade Federal de Uberlândia, Uberlândia, 2018.

GitHub".

A partir deste trecho, podemos observar que o principal requisito de segurança impactado foi a Disponibilidade destes websites. O interessante é que este tipo de ataque é realizado em dispositivos IoT, porém os impactos são em sistemas computacionais usuais, conforme observado neste trecho de Prado[11]:

"*Foram descobertos o uso de 49.657 (...) hospedeiros infectados pelo Mirai. Este número em sua maior parte é proveniente de câmeras de televisão de circuito fechado (...) inclui roteadores, gravadores digitais de vídeo e outros dispositivos da Internet das Coisas".*

Para entender quais vulnerabilidades foram exploradas, vamos referenciar outro trecho de Prado[12]:

"*Devido ao poder de processamento limitado desses dispositivos, muitos já possuíam vulnerabilidades e falhas de segurança de fábrica, sendo facilmente comprometidos e acessados de forma não autorizada".*

De forma mais específica, Prado[13] fornece um exemplo:

"*Produtos da empresa XiongMai especializada em fabricação de câmeras, que não permitiam a mudança da senha padrão de fábrica, e portanto sempre havia uma porta aberta para o acesso indevido de terceiros".*

Desta forma, a vulnerabilidade explorada está associada a configurações pad~rao de fábrica inseguras. Outra curiosidade referente a este ataque são a motivação de seus criadores, conforme descrito por Prado[14]:

11. PRADO, Marcelo Alves. *Análise experimental da botnet IoT Mirai*. 2018. 68 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de informação) - Universidade Federal de Uberlândia, Uberlândia, 2018.
12. PRADO, Marcelo Alves. *Análise experimental da botnet IoT Mirai*. 2018. 68 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de informação) - Universidade Federal de Uberlândia, Uberlândia, 2018.
13. PRADO, Marcelo Alves. *Análise experimental da botnet IoT Mirai*. 2018. 68 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de informação) - Universidade Federal de Uberlândia, Uberlândia, 2018.
14. PRADO, Marcelo Alves. *Análise experimental da botnet IoT Mirai*. 2018. 68 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de informação) - Universidade Federal de Uberlândia, Uberlândia, 2018.

"Os três jovens responsáveis pelo lançamento do Mirai - Paras Jha, Josiah White, e Dalton Norman - não tinham a intenção de derrubar a Internet, mas sim em obter vantagens no Minecraft, um jogo online de computador".

Isto mostra como, mesmo com motivações diferentes, a criação de um tipo de ataque para um determinado fim pode ser aproveitada por outros atacantes para realizar ataques com outras motivações.

Neste caso, seria importante agir junto aos fabricantes de dispositivos IoT para que as configurações de fábrica sejam passíveis de modificação, e que estas credenciais iniciais também tenham um nível maior de segurança associado. Por exemplo: ao invés de uma senha padrão para uma série de dispositivos, fornecer uma senha específica para cada dispositivo que pode vir junto ao manual de instrução do dispositivo.

10. CONCLUSÃO

O objetivo deste texto foi apresentar conceitos de segurança da informação e cibersegurança no contexto de Internet das Coisas (IoT). Estudos de caso foram utilizados para demonstrar como os conceitos de demandas de segurança (requisitos), pontos fracos existentes (vulnerabilidades), motivações dos atacantes, e possíveis estratégias a serem adotadas para elevar o nível de segurança (prevenção e detecção) podem ser úteis para fomentar uma análise de segurança de um sistema IoT. A seguir, são apresentadas algumas recomendações sobre como lidar com novos desafios de segurança em IoT para finalizar este capítulo.

Como considerações finais, devemos entender que há uma disputa sem fim entre atacantes e agentes de segurança. Sempre que há um novo mecanismo de segurança, atacantes trabalharão para quebrar este mecanismo. Quando este mecanismo for quebrado, agentes de segurança irão desenvolver um novo mecanismo, e assim por diante. Como visto no estudo de caso do Mirai, a comunidade de atacantes compartilha informações e ferramentas para execução de ataques, o que complica ainda mais tornar sistemas IoT seguros. A primeira provocação é se também é possível fomentar iniciativas para a divulgação de boas práticas, vulnerabilidades exploradas e ataques ocorridos de forma conjunta, ao invés de cada equipe de segurança de empresas tentar resolver seu problema de forma isolada.

Porém, com sistemas cada vez maiores e mais conectados pela Internet das

Coisas, é imprescindível entender que os ataques se tornam cada vez mais complexos. Ataques coordenados podem afetar requisitos diferentes em uma cadeia de ataques que busca distrair e espalhar esforços de equipes de segurança. Por exemplo: um ataque de indisponibilidade em um sistema IoT pode ser usado inicialmente para distrair a equipe de segurança da empresa responsável pelo produto, e depois um ataque para obter todos os dados dos usuários pode ser realizado. A segunda provocação que encerra este texto é sempre pensar na segurança desde a concepção dos sistemas IoT. Há oportunidades ao se adotar tecnologias emergentes como Internet das Coisas e Inteligência Artificial, porém é sempre essencial entender os novos desafios de segurança para suportar a transformação digital das empresas e sociedade de forma segura.

REFERÊNCIAS

ASHTON, Kevin et al. *That 'internet of things' thing*. RFID journal, v. 22, n. 7, p. 97-114, 2009.

CRUZ, Antonia Raiane Santos Araujo; GOMES, Rafael Lopes; FERNANDEZ, Marcial Porto. *DIMI: Detecção Inteligente de Botnets Mirai em Redes IoT*. Anais do Computer on the Beach, v. 12, p. 362-369, 2021.

DE MORAES, Alexandre; HAYASHI, Victor Takashi. *Segurança em IoT: Entendendo os riscos e ameaças em IoT*. Rio de Janeiro: Alta Books, 2021.

HAYASHI, Victor Takashi. *Non-invasive authentication for hands-free financial transactions in trusted connected locations*. 2022. Dissertação (Mestrado em Sistemas Digitais) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2022. doi:10.11606/D.3.2022.tde-21062022-140511.

HINTZBERGEN, Jule et al. *Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002*. Brasport, 2018.

MIESSLER, Daniel. *Securing the internet of things: Mapping attack surface areas using the OWASP IoT top 10*. In: RSA conference. 2015.

PRADO, Marcelo Alves. *Análise experimental da botnet IoT Mirai*. 2018. 68 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de informação) - Universidade Federal de Uberlândia, Uberlândia, 2018.

UMA ANÁLISE COMPARATIVA ENTRE A LEI DE SEGURANÇA CIBERNÉTICA CHINESA E A PROPOSTA EUROPEIA "*CYBER RESILIENCE ACT*"

Pedro Henrique Magalhães Lima

Mestrando em Direito pela Universidade Federal de Minas Gerais (UFMG). Pós-graduado em Direito Constitucional pela Universidade Anhanguera. Juiz Federal.

DOI: https://doi.org/10.59224/dti5.ch13

Resumo: No presente artigo faz-se uma análise comparativa entre a Lei de Segurança Cibernética da República Popular da China e a proposta de diretriz da União Europeia intitulada "Cyber Resilience Act" em quatro de seus aspectos: os atores envolvidos na aplicação, as entidades submetidas, as obrigações impostas e sanções imponíveis. Ao final, objetiva-se concluir sobre os pontos em que os documentos se assemelham ou trazem diferenças no tratamento dos quatro pontos analisados.

Palavras-chave: Segurança cibernética; Regulamentação.

Abstract: *In this paper a comparative analysis is done between the Cybersecurity Law of the People´s Republic of China and the European Union proposal "Cyber Resilience Act" in four aspects: entities enforcing the application of the normatives, entities subject to them, obligations, and possible sanctions. In the conclusion, the author aims to conclude about in what aspects the documents have similarities or differences.*

Keywords: *Cybersecurity; Regulation.*

Sumário: 1. Introdução; 2. Os Atores Envolvidos; 3. Critérios Adotados para a Seleção de Entidades Submetidas; 4. Obrigações e Procedimentos impostos; 5. Fiscalização e Sanções; 6. Alguns aspectos de maior debate: semelhanças e diferenças; 7. Situação atual da proposta europeia; 8. Conclusão; Referências.

1. INTRODUÇÃO

Neste artigo objetiva-se uma análise comparativa entre a Lei de Segurança Cibernética da República Popular da China[1] e a proposta diretriz de segurança cibernética da União Europeia (*European Union Cyber Resilience Act*[2]), formalizada em novembro de 2021, ainda em processo de aprovação. Pretende-se verificar se, e em quais pontos as duas normativas se aproximam, em quais se afastam, analisando-se determinados institutos comuns, os pontos que geram maior debate nos citados documentos.

As duas regulamentações surgem do mesmo contexto global de expansão da utilização da *internet* para a realização de negócios e transações entre pessoas localizadas nos mais diversos lugares do mundo, de aumento na utilização de equipamentos de internet das coisas (IoT), do surgimento e uso em larga escala de computação em nuvem, análises de big data, e da fácil transmissão de informações pessoais e comerciais sensíveis.

Esta realidade facilitou transações e o acesso a produtos e serviços, aumentou a interdependência entre os mercados de diversos Estados, e assim como o fluxo de informações, inclusive sensíveis, entre atores do mercado.

Na mesma medida, foi aberto grande espaço para ameaças cibernéticas, que aumentaram em número, magnitude, sofisticação, frequência e impacto. Ameaças ou ataques cibernéticos que façam interromper serviços e processos produtivos ganham potencial para gerar efeito cascata, resultando em impactos de longo alcance temporal e territorial.

Este o contexto do surgimento da lei chinesa e da proposta da União Europeia.

A lei da República Popular da China entrou em vigor em 1º de junho de 2017. Elenca, como seus objetivos (artigo 1º): assegurar a segurança cibernética, salvaguardar o espaço cibernético, a soberania, a segurança nacional, os interesses sociais e público, proteger os direitos dos cidadãos, pessoas jurídicas e organizações,

1. China. *Cybersecurity Law of the People's Republic of China*, disponível em <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>
2. EU. *Cyber Resilience Act* (Proposta 2021).

promover o desenvolvimento e a informatização saudáveis da economia e da sociedade. A lei é aplicável à construção, operação, manutenção e uso de redes, assim como à supervisão e gerenciamento de segurança cibernética no território chinês (artigo 2º).

A diretriz da União Europeia foi proposta em novembro de 2021, na gestão holandesa da Comissão da União Europeia, de Ursula von der Leyen.

No âmbito da União Europeia a atual regulamentação sobre segurança cibernética, Diretriz UE n. 1.148/2016, deixa discricionariedade para cada Estado, e consequentemente há grande variabilidade de requisitos de segurança. Esta variabilidade torna mais difícil o desenvolvimento de atividades econômicas no mercado da União Europeia, acabam por resultar em fragmentação do mercado, o que contraria parte da razão de ser da União, e pode gerar perdas financeiras e reduzir a confiança de fornecedores e consumidores.[3]

Diante desse contexto, pretende-se, além de elevar o nível de segurança cibernética no grupo, torná-lo uniforme, tendo em vista que uma vulnerabilidade, ou incidente, em qualquer país membro, num contexto de mercado globalizado, pode colocar a perder um número incalculável de interesses de cidadãos e organizações, privadas ou públicas.

Adiante, portanto, foram selecionados alguns elementos tratados em ambos os documentos. São eles os atores envolvidos, as entidades que se submetem às normas comentadas, os tipos de obrigações e procedimentos impostos, e, por fim, as sanções em caso de descumprimento.

2. OS ATORES ENVOLVIDOS

A Lei de Segurança Cibernética chinesa, por ser um documento editado por um só estado e para vigência neste estado, não há envolvimento específico de entidades internacionais ou supranacionais. Faz-se menção, porém, no artigo 7, que a China manterá intercâmbio de informação e cooperação internacionais nas áreas de governança do ciberespaço, pesquisa e desenvolvimento de tecnologia de rede, formulação de padrões, e, combate ao crime cibernético e à ilegalidade.

3. UE. *Cyber Resilience Act* (Proposta 2021), p. 9.

Quanto ao mais, todos os atores citados na lei são estatais ou privados, sejam eles pessoas físicas ou jurídicas.

Inicialmente é necessário atentarmos para o fato de que a China possui cinco níveis de governo: central, provincial, municipal, de condado, e, de vila. Em nível nacional (central), o Congresso Nacional Popular e seu Comitê são os órgãos legislativos máximos, e o Conselho de Estado, com seus ministérios, são o topo do Poder Executivo.[4]

As entidades governamentais responsáveis pelo planejamento, padronização, coordenação, supervisão e aplicação da lei são denominadas, genericamente, de departamentos, que podem compor quaisquer das cinco esferas de governo. São estes departamentos que recebem, de quaisquer indivíduos ou organizações, denúncias de condutas que podem colocar em risco a segurança cibernética, das informações e telecomunicações (art. 14). Aos departamentos também devem ser reportados, pelos agentes supervisionados, quaisquer falhas ou vulnerabilidades (arts. 22 e 25).

Os departamentos do Conselho de Estado, órgão máximo do Poder Executivo nacional, para telecomunicações e segurança pública são responsáveis pela supervisão, padronização e gerenciamento gerais (arts. 8 e 15). As demais esferas de governo têm, igualmente, departamentos envolvidos na aplicação das normas de segurança cibernética chinesa (art. 16).

Já no âmbito da proposta de diretriz da União Europeia, pela natureza supranacional da organização, envolvem-se na sua aplicação tanto órgãos da União Europeia, entidades não diretamente submetidas a um estado membro, quanto aqueles dos estados membros, e agentes privados.

Quatro são os órgãos da União Europeia: a Comissão da União Europeia, a Agência da União Europeia para Segurança Cibernética (ENISA), o Grupo de Cooperação, e a Rede Europeia de Intermediação de Crises Cibernéticas (EU-CyCLONe).

A Comissão da União Européia é o órgão político da União Europeia que toma decisões executivas, formula políticas e propõe diretrizes e normas. É formado por comissários representantes dos países que compõem a União Europeia.

4. LIU, Wei; JAMES, Toby S.; MAN, Caixia. *Governance and public administration in China, Policy Studies*. 2002, 43:3, p. 389.

A ENISA (artigo 6º) presta assistência aos Estados Membros na formulação da estratégia nacional, mantém o registro europeu de vulnerabilidades, com a descrição da vulnerabilidade, o produto ou serviço afetado e a severidade. Além disso, deve editar, bienalmente, um relatório sobre o estado de segurança cibernética da União Europeia.

O Grupo de Cooperação (artigo 12) é formado por representantes dos Estados Membros, da Comissão da União Europeia e da ENISA. O Grupo congrega as funções de orientação às autoridades competentes de cada Estado na implementação da diretriz, assessoramento da Comissão quanto a novas iniciativas, e funciona como um foro para troca de boas práticas e informações entre estados. É, ainda, o Grupo que estabelecerá metodologia de aprendizado por pares, rodadas conduzidas por *experts* em segurança cibernética indicados pelos Estados Membros, de participação facultativa por estes.

A Rede Europeia de Intermediação de Crises Cibernéticas (EU-CyCLONe, artigo 14) é composta por representantes das autoridades competentes de cada Estado-membro, e dela a Comissão da União Europeia participará como ouvinte. Terá como função apoiar o gerenciamento de incidentes cibernéticos de larga escala e crises, no aspecto operacional, garantir a troca de informações entre Estados Membros e União Europeia, avaliar os impactos de incidentes de larga escala e propor medidas de mitigação.

Neste ponto passamos a estudar as funções dos Estados-membros, assim como de seus órgãos internos. Os Estados-membros são responsáveis por adotar uma estratégia nacional de segurança cibernética, nela se inclui, em linhas gerais: objetivos e prioridades em segurança cibernética, estrutura de governança, cooperação entre os setores público e privado e cooperação entre autoridades competentes sobre a diretriz.

Internamente cada Estado-membro deve ter: um ponto único de contato, autoridades competentes, CSIRT, e, Rede de CSIRT.

O ponto único de contato de cada Estado-membro ficará responsável por coordenar questões ligadas à segurança de rede e sistemas de informação, assim como cooperação além das fronteiras do estado no âmbito da União Europeia.

As autoridades competentes, que são, em verdade, órgãos, podendo ser um ou mais de um, são designados pelos Estados-membros e têm competência para

gerenciamento de incidentes e crises de larga escala, assim como para supervisionar as entidades submetidas à diretriz.

Os Grupos de Resposta a Incidentes de Segurança Computacional (CSIRT - Computer Security Incident Response Team, artigo 10 da diretriz) são órgãos técnicos, instituídos por cada Estado-membro, que poderão, ou não, integrar o corpo das autoridades competentes. Os Grupos irão desempenhar tarefas técnicas no monitoramento de ameaças e tratamento de incidentes, coordenar a revelação de vulnerabilidades. Cidadãos e pessoas jurídicas poderão reportar aos CSIRTs sobre vulnerabilidades, e estes devem acompanhar o incidente ou ameaça notificada.

Por fim, os diversos CSIRTs de cada Estado-membro compõem a Rede de CSIRTs (artigo 13), vocacionadas a promover a rápida cooperação operacional, com a troca de informações sobre incidentes, ameaças, riscos, vulnerabilidades, e, de soluções técnicas e boas práticas.

3. CRITÉRIOS ADOTADOS PARA A SELEÇÃO DE ENTIDADES SUBMETIDAS

Conforme se verá mais adiante em tópico apartado, principalmente a norma chinesa é bastante criticada por sua vagueza, tendo sido necessária a atuação de doutrinadores chineses e estrangeiros com o objetivo de aclarar a interpretação de alguns pontos.

Analisando-se a norma chinesa, é possível verificar que ela submete dois grandes grupos de entidades: os operadores de rede (a que se referem os arts. 9º, 21, 24, 25, 28, 29, 40 a 43, 47, 49, 50, 55, 59, 61, 64, 68, 69, 72 e 76) e; operadores de infraestrutura de informações críticas (referidos nos arts. 34 a 38, 59, 65, 66).

O critério utilizado pela lei chinesa, para a imposição das diversas obrigações que elenca, foi do tipo de serviços prestados. O artigo 76, sucintamente, define "network operators": "*Article 76: The language below has the following meanings in this law: (...) (3) "Network operators" refers to network owners, managers, and network service providers.*"

Nenhuma definição é dada sobre quais entidades se enquadram como operadores de infraestrutura de informações críticas. Assim sendo, buscando-se na própria lei

elementos para a definição, tem-se, inaugurando a Seção 2, sobre segurança de operações em infraestrutura de operações críticas, tem-se o art. 31[5] que trata da proteção de alguns setores sensíveis, quais sejam, serviços de comunicações e informações, energia, tráfego, recursos hídricos, finanças, serviços públicos, governo eletrônico, e outras infraestruturas de informações que, se destruídas, não operativas, ou sujeitas a vazamento, poderiam comprometer seriamente a segurança nacional, o bem estar nacional ou o interesse público.

Passando-se à análise dos critérios utilizados pela proposta de diretriz da União Europeia, tem-se que as entidades submetidas foram divididas em dois grandes grupos: entidades essenciais e entidades importantes. Para tanto, via de regra, a proposta se utiliza dos critérios porte e setor.

Quanto ao porte, a proposta faz remissão à Recomendação 361/2003 da União Europeia. São microempresas aquelas que empregam menos de 10 pessoas, e têm receita anual não superior a 2 milhões de euros, pequena empresa as que empregam menos de 50 pessoas, e têm receita anual não superior a 10 milhões de euros, e, médias as que empregam menos de 250 pessoas, e têm receita anual não superior a 50 milhões de euros.

Tendo em mente a gradação do porte das empresas, destacada acima, submeter-se-ão à diretriz, se aprovada, as entidades, públicas ou privadas, de médio porte ou maiores, que atuam nos setores de energia, transporte, bancário, infraestrutura de mercado financeiro, saúde, recursos hídricos, infraestrutura digital, gerenciamento de tecnologia da informação e comunicação, algumas entidades da administração pública, espacial, correios e *courier*, gerenciamento de lixo, química, alimentícia, manufatura de alguns produtos e provedores de serviços digitais. Além disso, ainda serão submetidas, independentemente do porte, os Provedores de redes de comunicação, ou serviços de comunicação disponíveis publicamente, registradores de

5. "Article 31: The State implements key protection on the basis of the cybersecurity multilevel protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure."

domínio de alto nível, fornecedor único de serviço fundamental para a manutenção de atividades econômicas ou serviços sociais essenciais, fornecedor de serviço cuja interrupção possa causar significativo impacto na segurança ou saúde pública, ou causar risco sistêmico em setor que tenha impacto além-fronteiras, e, entidades da administração pública.

Entre estas, são consideradas entidades essenciais aquelas que: excedam o limite para caracterização como entidade média e atuem nos setores de energia, transporte, bancário, infraestrutura de mercado financeiro, saúde, recursos hídricos, infraestrutura digital e espacial; entidades médias provedores de redes de comunicação ou de serviços de comunicação disponíveis publicamente, e; independentemente do porte, os registradores de domínio de alto nível e entidades da administração pública.

A segunda categoria de entidades tratadas pela proposta são das entidades importantes: entidades de porte médio que atuem nos setores de energia, transporte, bancos, infraestrutura de mercado financeiro, saúde, recursos hídricos, infraestrutura digital, gerenciamento de tecnologia da informação e comunicações, administração pública e espacial; que ultrapassem o limite de porte médio dos setores postal, courier, gerenciamento de lixo, química, alimentícia, manufatura de alguns produtos e provedores digitais; de micro e pequeno porte provedores de redes públicas de comunicação e serviços de comunicação disponíveis publicamente, e; de micro e pequeno porte classificadas pelos estados membros como importantes.

Conforme artigo 30 (1), o efeito prático da distinção entre entidades essenciais e importantes está em que estas se submetem a fiscalização posterior.

Por fim, a proposta expressamente ressalva de sua aplicação as entidades que desenvolvem atividades nas áreas da defesa, segurança nacional e pública, os poderes Judiciário e Legislativo, e, bancos centrais. Além disso, igualmente não estarão sujeitas às normas europeias nenhuma entidade quando a sujeição contrariar os interesses de defesa, segurança pública e nacional.

4. OBRIGAÇÕES E PROCEDIMENTOS IMPOSTOS

Destaca-se aqui algumas obrigações a que se submetem as entidades submetidas à norma chinesa.

Sobre a categoria operadores de rede, o artigo 21 impõe a formulação de sistemas de gerenciamento da segurança interna, a adoção de medidas para prevenir a ocorrência de vírus, ataques e intrusões adoção de medidas de monitoramento e gravação do status da rede, com necessidade de arquivamento dos *logs* de dados, classificação de dados e *backup* de dados importantes. No caso de detecção de vulnerabilidades, devem imediatamente adotar medidas para remediá-las, além de informar os usuários e os departamentos competentes. Em caso de incidentes de segurança, a adoção de um plano de resposta emergencial deve ser imediatamente realizada (artigo 25).

Acerca dos dados coletados pelos operadores de rede, estes estão proibidos de revelá-los, neles interferir, ou fornecer a outros, tomando medidas para evitar que vazem, se percam ou sejam destruídos (art. 42).

Já sobre a categoria dos operadores de infraestrutura de informações críticas pesam obrigações mais gravosas. Devem contar com grupos especializados de gerenciamento de segurança para conduzir checagens de segurança, periodicamente devem conduzir treinamento técnico e avaliações de habilidade dos empregados, contar com *backups* de recuperação em caso de desastres, formular planos emergenciais de resposta, entre outras obrigações que constarem de outras normas (artigo 34).

Quaisquer equipamentos de rede, utilizados pelos operadores de infraestrutura de informações críticas, que possam impactar a segurança nacional, devem passar por uma revisão de segurança por departamentos do Conselho de Estado (artigo 35).

Operadores de infraestrutura de informações críticas que coletem ou produzam informações pessoais no território chinês devem, necessariamente, mantê-los em servidores fisicamente mantidos em território chinês (artigo 38).

Por fim, destaca-se o artigo 39, que impõe aos departamentos estatais as seguintes de proteção à segurança das infraestruturas de informações críticas (e consequentemente seus operadores): condução de checagens pontuais; retenção de serviços para condução de testes; periodicamente impor aos operadores exercícios de resposta incidentes; e promoção de suporte técnico e assistência no gerenciamento e recuperação em caso de incidentes.

Já com relação à norma Europeia, em linhas gerais, as obrigações impostas podem ser divididas entre obrigações de governança (artigos 17 e 18) e obrigações de notificação (artigo 20).

Relativamente às primeiras, os órgãos de administração das entidades devem aprovar medidas de gerenciamento de risco cibernético, e os gestores (pessoas físicas) podem ser responsáveis em caso de não conformidade com a diretriz, sem prejuízo da responsabilidade pelo descumprimento de leis nacionais sobre o mesmo tema.

Regularmente a gerência das entidades devem se submeter a treinamentos na área, a fim de estarem atualizados com o conhecimento e melhores práticas sobre o tema da segurança cibernética em cada setor.

Além disso, as entidades devem tomar algumas medidas técnicas e organizacionais com vistas ao incremento da segurança, como o desenvolvimento de análise de risco sobre suas atividades e setor em que atuem, prevenção, detecção, resposta e recuperação em caso de incidentes, continuidade de prestação do serviço durante o gerenciamento da crise, contribuição para a segurança da cadeia produtiva, e utilização de criptografia.

Se submetem, ainda, às obrigações de notificação em caso de ameaça ou incidente que tenha ou possa ter impacto na continuidade da prestação de serviços. Nestas situações devem notificar a(s) autoridades(s) competentes e o CSIRT de seus estados, que deverão receber a notificação inicial, responder à entidade notificante, inclusive com orientações e sugestão de possíveis medidas para mitigação do (eventual) impacto. Serão, também, notificados, os tomadores dos serviços (clientes) das que podem ser afetados, informando medidas que possam ser tomadas em resposta ao incidente ou ameaça.

O procedimento da notificação envolve três fases. A primeira, da notificação inicial, que se dá em 24 horas após o conhecimento do incidente ou ameaça. A segunda, sob requisição da autoridade competente ou CSIRT, deve ser enviado um relatório intermediário sobre atualizações relevantes sobre o caso. E a terceira e última, do relatório final, que deverá acontecer em até um mês após a notificação inicial, com a descrição detalhada do incidente, e seu impacto, o tipo de ameaça ou causa que possivelmente o desencadeou, e, medidas de mitigação aplicadas e em execução.

5. FISCALIZAÇÃO E SANÇÕES

A norma chinesa defere aos departamentos estatais a incumbência de fiscalização

das entidades operadoras de rede ou de infraestrutura de informações críticas.

As sanções aplicáveis (artigos 59 a 75), no documento chinês, são diretamente correspondentes a cada uma das obrigações impostas. As sanções previstas são: ordens de correção; advertências; multas, tanto à entidade, quanto à pessoa incumbida da gerência; suspensão temporária de operações; suspensão do negócio para correções; fechamento de *websites*; cancelamento de permissões ou licenças para os negócios; e, detenções (não criminais) que podem ir de 5 a 15 dias.

No âmbito da possível futura regulamentação europeia, o monitoramento e a tomada de medidas necessárias para assegurar o cumprimento da diretriz cabe às autoridades competentes de cada Estado-membro, e a supervisão é realizada com base no enfoque sobre o risco (artigo 28, 1).

As atividades de supervisão sobre entidades essenciais envolvem inspeções em sítio, remotas e fiscalizações randômicas, auditorias sobre segurança regulares, requisição de informações, acesso a dados e documentos, exigência de demonstração de implementação de políticas de segurança cibernética (artigo 29, 2).

Diversas são as ferramentas de coerção disponíveis, quais sejam: aplicação de advertências em caso de não conformidade com as obrigações da diretriz; instruções ou ordens vinculantes, requisitando que as entidades solucionem deficiências ou infringência à diretriz; ordem de cessar conduta; ordenar que entidades informem a pessoa jurídica ou física para quem prestam serviços que são potencialmente afetadas por ameaça cibernética; ordenar que entidades tornem pública não conformidades com a diretriz.

Em caso de, apesar da aplicação de medidas de coerção, haver renitência na não observância da diretriz, serão cabíveis as seguintes sanções: imposição ou requerimento de imposição de multas administrativas, suspensão ou requisição de suspensão de certificação ou autorização relativamente a parte dos serviços ou todos os serviços ou atividades desenvolvidas pela entidade; suspensão ou requisição de suspensão de banimento temporário contra pessoa com responsabilidade gerencial pelo descumprimento (artigo 29, 5).

As sanções serão sempre temporárias, enquanto durar o descumprimento, e não se aplicam a entidades da administração pública.

Limitando a ação dos Estados-membros no procedimento de aplicação das

sanções, a proposta de diretriz exige que, antes, seja respeitado o direito de defesa, e que as entidades sejam notificadas sobre as conclusões preliminares, com tempo razoável para resposta. No caso de se concluir pela sanção, na dosimetria, há que se levar em conta a repetição ou não da infração, falha na notificação ou na solução de incidentes de larga escala, duração da infringência; danos acusados ou potenciais danos; dolo ou culpa; medidas tomadas para evitar ou mitigar os danos; aderência a códigos de conduta aprovados ou certificações (artigo 29, 8).

Relativamente às entidades importantes, a diferença quanto à supervisão, como já se disse, é o fato de não ser possível inspeção anterior randômica. As ferramentas de suporte à aplicação da diretriz continuam sendo as mesmas aplicáveis às entidades essenciais, e igualmente o tipo das sanções, sendo estas modificáveis, portanto, tão somente na dosimetria.

6. ALGUNS ASPECTOS DE MAIOR DEBATE: SEMELHANÇAS E DIFERENÇAS

A norma chinesa, desde sua entrada em vigor, vem sendo criticada em diversas de suas disposições. Passa-se, então, à análise sobre algumas semelhanças e diferenças das duas normas em estudo.

O primeiro ponto que merece destaque é o delineamento dos órgãos competentes para a aplicação das duas regulamentações.

A norma chinesa defere a departamentos das cinco esferas de governo a competência para a aplicação. Porém, não há um delineamento claro das competências dos numerosos departamentos citados, na própria lei, o que fica relegado a diplomas normativos de hierarquia inferior[6].

6. Cite-se, como exemplo, os seguintes dispositivos (grifos nossos): "Article 8: State cybersecurity and informatization departments are responsible for comprehensively planning and coordinating cybersecurity efforts and related supervision and management efforts. The State Council departments for telecommunications, public security, and other relevant organs, are responsible for cybersecurity protection, supervision, and management efforts within the scope of their responsibilities, *in accordance with the provisions of this Law and relevant laws and administrative regulations*. Cybersecurity protection, supervision, and management duties for relevant departments in people's governments at the county level or above *will be determined by relevant national*

Neste ponto, é interessante notar a crítica feita por Wei Liu, Toby S. James & Caixia Man, acerca do sistema de tomadas de decisões administrativas na China, que o compara a um "favo de mel"[7].

Na proposta europeia, por certo que não descendo a minúcias relativamente à organização interna dos órgãos estatais (em razão da própria limitação que a soberania dos Estados-membros traz), é de se concluir que o projeto delineia com mais clareza as competências de cada ator envolvido na sua aplicação.

Quanto à definição das entidades submetidas, é possível notar que a norma chinesa não define de forma clara quais se enquadram em cada categoria.

Como se disse linhas acima, a definição sobre o que sejam operadores de infraestrutura de informações críticas não é dada pela norma, sendo necessário esforço para a inferência do sentido da norma através de interpretação sistemática, com o auxílio do que dispõe o artigo 31, já citado.

Este artigo se vale de termos relativamente vagos, como "segurança nacional", "bem estar nacional" e "interesse público", e quaisquer entidades que, enquadradas como operantes de setores que impactem tais critérios, poderiam ser submetidas à regulamentação mais restrita, o que gera certa insegurança jurídica.

Em razão da indefinição referida, o governo da Nova Zelândia, quando da edição da lei chinesa, elaborou documento direcionado aos empreendedores neozelandeses que operavam na China, informando que não havia definição do que seria operadores de infraestrutura de informações críticas, de forma que empreendimentos de outros setores que não fossem telecomunicações poderiam, ainda assim, serem afetados

regulations.

7. "Decision making in China is characterized as a disjointed, protracted, and incremental process with state and non-state actors involved. It is fragmented over a honeycomb-liked administrative system in which cross-level and cross-sectoral bureaucracies bargain and negotiate for their own interests in the policy battlefield. (...) Moreover, local officials at each level are not "string dolls" that only implement policies from a top-down discipline; rather, they react as policy entrepreneurs who adopt new goals or alter policy instruments drawing from practical experience or policy experiments in specific local contexts. To this end, adaptive policies are initiated across the country to accommodate regional varieties and local flexibilities." Wei Liu, Toby S. James & Caixia Man (2022) *Governance and public administration in China, Policy Studies*, 43:3, p. 390/391.

por requisitos mais rigorosos.[8] Ainda neste mesmo sentido, em matéria publicada no *Center for Strategic & International Studies*, arguiu-se sobre uma deliberada ambiguidade da norma chinesa, quando em comparação com normas europeias.[9]

Na busca de definição para o termo, Jyh Na-Lee, professor associado da Faculdade de Direito da Universidade Chinesa de Hong Kong, aduz que infraestrutura crítica se refere a sistemas e redes que são social e economicamente cruciais ao funcionamento de um país, em termos de como bens e serviços são essenciais para a segurança nacional, vitalidade econômica, segurança e saúde dos cidadãos.[10]

Contudo, em que pese as críticas ao documento chinês, também é possível encontrar na proposta europeia dispositivos que abrem certa discricionariedade na submissão, ou não submissão, de entidades à norma. Cita-se, por exemplo, o artigo 2 bis (1) "vii" e "viii", e, (2) "iv", que permitem aos Estados-membro a classificação de certas entidades médias e pequenas como essenciais, e pequenas e microempresas como importantes. Além disso, utilizando-se dos termos relativamente abertos "interesses de defesa" e "segurança pública e nacional", a norma pode ser inaplicável quando colocar em risco aqueles valores (artigo 2, 3aaa).

Relativamente às obrigações impostas, nota-se que ambos documentos dão grande importância às obrigações de notificações, tanto às autoridades competentes para a fiscalização, quanto aos usuários possivelmente afetados por vulnerabilidades e incidentes.

Porém, e neste ponto afastando-se da clareza encontrada na normativa europeia quanto às obrigações, é possível encontrar na norma chinesa ausência de definições

8. "There is currently no fixed definition of the term "critical information infrastructure operator". This means that organisations operating in sectors removed from telecommunications infrastructure could still be impacted by the law's more stringent requirements." Nova Zelândia. Understanding China´s Cybersecurity Law. 2017. Disponível em<https://www.ncsc.govt.nz/assets/NCSC-Documents/Understanding-Chinas-cybersecurity-law.pdf>, acesso em 02/07/2022.
9. MARANTO, Lauren. *Who benefits from China´s Cybersecurity laws?*. 2020. Disponível em <https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws>. Acesso em 02/07/2022.
10. LEE, Jyh-An. *Hacking into China's Cybersecurity Law*. Wake Forest L. Rev., v. 53, p. 57, 2018, disponível em < http://www.wakeforestlawreview.com/wp-content/uploads/2019/01/w05_Lee-crop.pdf>

claras, em alguns aspectos, assim como o tratamento de forma pouco sistematizada. Algumas disposições são bastante claros sobre as obrigações impostas, e outros bastante genéricos, com a utilização de termos vagos ou remissão a outras normas, como é o caso do artigo 9º[11].

Acerca da vagueza redacional encontrada no documento chinês em estudo, é interessante notar o que ensina Liudmyla Balke, no sentido de que os críticos às normativas chinesas sustentam ser comum, naquele país, a utilização de termos extremamente vagos nas redações das legislações, de forma a dar flexibilidade aos formadores de políticas públicas.[12]

Por fim, quanto às sanções, as duas normas se aproximam na medida em que permitem a imposição de advertências, multas (inclusive a pessoas físicas incumbidas da gerência de entidades, suspensões temporárias de licenças e negócios.

Porém, é de se destacar que o documento chinês permite medidas mais duras. Enquanto a proposta europeia expressamente dispõe que as sanções são sempre temporárias, a lei de segurança cibernética da china permite a imposição de sanções definitivas, como o cancelamento de permissões ou licenças, além de detenção não criminal de pessoas, que podem ser de 5 a 15 dias.

7. SITUAÇÃO ATUAL DA PROPOSTA EUROPEIA

A proposta europeia esteve, recentemente, de 16 de março a 25 de maio de 2022, sob consulta pública, que pretendeu congregar as opiniões de representantes de entidades submetidas, de autoridades dos Estados-membro incumbidas de preservação de segurança cibernética, consumidores, entidades de avaliação de conformidade, acadêmicos e público em geral. Buscou-se, com isso, conhecer os problemas atuais e possíveis problemas futuros relacionados com a segurança cibernética de produtos e

11. "Article 9: Network operators carrying out business and service activities must follow laws and administrative regulations, respect social morality, abide by commercial ethics, be honest and credible, perform obligations to protect cybersecurity, accept supervision from the government and public, and bear social responsibility."
12. BALKE, Liudmyla. *China's new cybersecurity law and US-China cybersecurity issues*. Santa Clara L. Rev., v. 58, p. 137, 2018, disponível em <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2849&context=lawreview>

serviços digitais, assim como delinear estratégias para a resolução de eventuais problemas e seus impactos. [13]

A consulta pública teve um total de 167 comentários válidos recebidos, sendo que, destes, 35,3% foram de empresas e organizações empresariais, 28,1% de associações empresariais, e, 13,1% de entidades públicas. Cidadãos, organizações de consumidores e universidades responderam, juntos, por 11,98% das opiniões válidas.

Agora o projeto seguirá para deliberação sobre sua adoção, pela Comissão, prevista para o terceiro trimestre de 2022.

8. CONCLUSÃO

Cotejando os dois documentos, nos quatro pontos de contato selecionados, quais sejam, os atores envolvidos em suas aplicações, as entidades submetidas, as obrigações impostas e as sanções cabíveis em caso de descumprimento, é de se concluir que o aspecto em que mais se aproximam é na definição de sanções.

Várias das sanções aplicáveis são semelhantes, e o documento chinês, neste aspecto contando com satisfatória definição, ultrapassa a proposta europeia relativamente à duração das sanções, que poderão ser permanentes, e na possibilidade de detenção àquelas pessoas físicas que fizerem descumprir a normativa.

Nos aspectos atores envolvidos na aplicação, entidades submetidas e obrigações impostas, de fato observou-se, na normativa chinesa, considerável grau de indefinição, algumas vezes pela utilização de termos vagos (como no caso do artigo 9º), outras vezes por realmente não especificar (como é o caso das competências entre departamentos das cinco esferas de governo). Já no documento europeu, relativamente a estes três aspectos, observou-se que a regra foi a clareza redacional, liberando-se aos Estados-membros pequeno grau de discricionariedade, tal como na inclusão de entidades que, via de regra, não seriam abrangidas pelas obrigações da diretriz.

13. Disponível em <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/public-consultation_pt>

REFERÊNCIAS

BALKE, Liudmyla. *China's new cybersecurity law and US-China cybersecurity issues*. Santa Clara L. Rev., v. 58, 2018.

CHINA. *Cybersecurity Law of the People's Republic of China*.

EU. *Cyber Resilience Act* (Proposta 2021).

LEE, Jyh-An. *Hacking into China's Cybersecurity Law*. Wake Forest L. Rev., v. 53, 2018.

LIU, Wei; JAMES, Toby S.; MAN, Caixia. *Governance and public administration in China, Policy Studies*. 2002.

MARANTO, Lauren. *Who benefits from China´s Cybersecurity laws?*. 2020.

NOVA ZELÂNDIA. *Understanding China´s Cybersecurity Law*. 2017.

TELECOMUNICAÇÕES E SUA RELAÇÃO COM A IOT

Débora Batista Araújo

Fellow of Information Privacy – IAPP; Certificações CIPP/E, CIPM – IAPP; Data Protection Officer certificada pela Universidade de Maastricht; Especialista em Direito da Economia e da Empresa – FGV/SP; Especialista em Direito Societário – Insper; Especialista em Direito Contratual – PUC/SP; Cursando LL.M em Privacidade, Cybersegurança e Gerenciamento de Dados, pela Universidade de Maastricht (conclusão 2023). Advogada.

DOI: https://doi.org/10.59224/dti5.ch14

Resumo: As novas funcionalidades de gerenciamento da rede de telefonia celular trazidas pelo 5G permitem segmentação de rede, virtualização e desvinculação entre hardware e software, de maneira a praticamente criar várias redes dentro de uma só. Este é um importante habilitador dos casos de uso da Internet das Coisas. Isso traz também desafios relacionados com a mudança na atuação de cada *stakeholder* do ecossistema de conectividade, demandando olhar atento a respeito do papel de cada um e das consequências de mercado e geopolíticas. O presente artigo discorre sobre a novel forma de conexão entre dispositivos, ao passo que busca ilustrar os desafios decorrentes da abertura, a vários *players*, do acesso às redes de telecomunicações (o Open RAN – Radio Access Network).

Palavras-chave: Internet das Coisas, 5G, Open RAN.

Abstract: *The 5G new mobile network management functionalities enable network segmentation, virtualization and software/hardware decoupling, in a way that virtually creates many networks in a single one. These are important enablers of the Internet of Things. Such new features also come with challenges related to the changes in each stakeholder´s role in the connectivity ecosystem, requiring an attemptive look with regard to the market and geopolitical consequences of such changes. The presente article discusses such new connection between devices and at the same time, attempts to illustrate the challenges related to the opening of access to telecommunication networks to different players (the Open RAN – Radio Access Network).*

Keywords: *Internet of Things, 5G, Open RAN.*

---

1. INTRODUÇÃO

A ITU - International Telecommunication Union, agência especializada das Nações Unidas para Tecnologia da Informação e Comunicação, escreveu, em 2005, relatório sobre a Internet das Coisas ("IoT"). Mencionou que o acesso à banda larga mudou a natureza da internet, fazendo derreter os fluxos de receita por transmissão de voz e destacou que, se a tendência continuasse, a internet se tornaria uma plataforma para transmissão de dados entre coisas e não somente entre humanos[1].

Na análise de então, a ITU destacava o aumento da velocidade da internet como relevante habilitador do IoT, juntamente com o desenvolvimento das novas tecnologias, como o RFID – *Radio-frequency identification* (que já não era tão nova assim). Esses elementos estabeleceriam novas possibilidades de criação de produtos e serviços a serem vendidos aos consumidores, em um mercado que dava mostras de saturação nos países desenvolvidos.

As redes móveis estavam em sua terceira geração e falava-se na relevante transformação que consistia em ter a conectividade ao alcance da mão, dada a aumentada qualidade de transmissão em dispositivos móveis, e na importância das gerações futuras de redes de telecomunicações (*NGN – Next Generation Networks*).

Hoje, os padrões de funcionalidade de redes móveis aprovados pelo 3GPP[2] estão

1. ITU – International Telecommunication Union. *The Internet of Things*. Geneva, 2005. (ITU Internet Reports 2005), p. 5. Disponível em: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf. Acesso em: 08/12/2022.
2. O 3GPP, sigla para 3rd Generation Partnership Project, é uma organização criada em 1998 por 7 organizações de desenvolvimento de padrões em telecomunicações (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), conhecidas como "Parceiros Organizacionais", para estabelecer padrões globais para a evolução da rede de telecomunicações, orientados à indústria e viabilizando a interoperabilidade e a atuação multi-fornecedores para implementação. Originalmente criada para estabelecimento dos padrões que viabilizariam a transição da rede GSM (2G) para a 3G, é responsável pelas *releases* que determinam a evolução da tecnologia e as novas gerações de rede de telefonia celular. Da *release* 15 em diante, surgem os padrões do 5G, a telefonia celular de 5ª. Geração. Veja mais em: *Partnership Project Description*. Disponível em: https://www.3gpp.org/images/downloads/partnership-project-description.pdf. Acesso em: 12/01/2023. I*ntroducing 3GPP*. Disponivel em: https://www.3gpp.org/about-us/introducing-3gpp. Acesso em: 12/01/23.

na quinta geração e o 5G tem sido muito comemorado como elemento fundamental do IoT, uma vez que a baixa latência, alta velocidade e capacidade de conexão simultânea permitem manter as funcionalidades de múltiplos dispositivos devidamente operacionais, melhorando a vida dos consumidores[3].

É verdade que os benefícios do 5G ainda não são totalmente conhecidos hoje, uma vez que os casos de uso estão sendo desenvolvidos. Palatella et al[4]. lembram que a própria internet precisou de cerca de 10 anos para ser massivamente utilizada. De todo modo, a agência de análise de mercado IoT Analytics lembra que apesar de 2022 ter sido um ano de más notícias sob a ótica macroeconômica, o número de dispositivos conectados à Internet das Coisas cresceu para cerca de 14,4 bilhões e investimentos cresceram para um valor da monta de US$ 202 bilhões[5].

Para comportar tantos dispositivos, sensores e atuadores atuando simultaneamente na rede, bem como tantos casos de uso distintos, a conectividade é um elemento essencial, assim como a possibilidade de gerenciamento de redes de forma simplificada, de preferência por meio de softwares, tornando a solução mais leve como um todo.

Este artigo tem por objetivo trazer informações sobre o papel do 5G para a conectividade da Internet das Coisas, passando por suas inovações, benefícios e desafios, sem a pretensão, entretanto, de esgotar o tema, que comporta amplo debate por qualquer ponto de vista que se adote.

2. INTERNET DAS COISAS E AS TELECOMUNICAÇÕES

Para falar em Internet das Coisas, é importante pontuar que as relações entre os usuários e as coisas vêm mudando ao longo dos anos. Deixamos de simplesmente possuir produtos isolados, existentes em si mesmos, para passar a ter serviços que

3. MEIRA, Silvio. *23 anotações sobre 2023. 5G & Internet das Coisas*. Disponível em: https://silvio.meira.com/silvio/23-anotacoes-sobre-2023-x/ Acesso em: 09/01/2023
4. PALATELLA, Maria Rita et. al. *The Internet of Things in the 5G era: enablers, architecture and business models*. P. 13. Disponível em: https://ieeexplore.ieee.org/document/7397856 Acessado em: 12/11/2022
5. TAPARIA, Anand. *IoT 2022 in Review: The 10 Most Relevant IoT Developments of the Year*. Disponível em: https://iot-analytics.com/iot-2022-in-review/. Acesso em: 31/01/2023

são viabilizados por meio de determinados dispositivos. O valor que se extrai dos serviços decorre de estarem eles conectados em rede, adicionando informações e inteligência à experiência do usuário, sendo o produto, ou dispositivo, um instrumento que coleta as informações, na ponta do usuário.

Wentzel, citada por Magrani[6], destaca que se encontra em curso a 4ª Revolução Industrial, "*que se caracteriza essencialmente por uma internet ubíqua e móvel, por sensores e dispositivos cada vez mais baratos e menores e pelo desenvolvimento da inteligência artificial.*"

A Internet das Coisas, portanto, surge no contexto de mudança da relação dos indivíduos com as coisas, decorrentes da hiperconectividade e do volume crescente de dados gerados por essa conectividade onipresente, tratados de forma relacional (o Big Data)[7].

Meira[8] destaca 10 propriedades das coisas conectadas e ressalta, ainda, que as coisas, na Internet das Coisas, são Objetos Digitais Completos, por serem dispositivos com possibilidade de computação, comunicação e controle. Ausente qualquer um desses elementos, desnatura-se o Objeto Digital Completo e de Internet das Coisas

6. MAGRANI, Eduardo. *A Internet das Coisas.* Rio de Janeiro: FGV Editora, 2018. p. 79
7. *Op. Cit., p. 21*
8. "As coisas, conectadas, têm pelo menos dez propriedades [bit.ly/3Ff3JDD] que não estão associadas, hoje, ao seu fogão, moedor de café e fechadura da porta: [1] são identificáveis e endereçáveis, estão em rede; [2] são programáveis, mesmo as mais rudimentares; [3] têm memória, [4] sensores, pra capturar sinais ao seu redor, podem ter [5] atuadores, para agir sobre seu ambiente, [6] são rastreáveis, podemos saber onde estão e por onde estiveram… [7] podem estabelecer conexões com outras coisas, pessoas e organizações, assim como [8] relacionamentos, para formar redes, grupos, comunidades, onde poderão realizar [9] interações com outros agentes aos quais podem se [10] associar, para realizar tarefas mais complexas do que uma única coisa poderia." MEIRA, Silvio. *23 anotações sobre 2023 [x] – 5G & a internet das coisas.* Disponível em: https://silvio.meira.com/silvio/23-anotacoes-sobre-2023-x/. Acesso em: 09/01/2023.

não se deve falar.[9-10]

Importante destacar que uma das características da Internet das Coisas é a grande heterogeneidade – de dispositivos, de tecnologias, de conectividade. Para diferentes casos de uso, diferentes funcionalidades e conectividade são mais críticas. Para *smart homes*, por exemplo, torna-se relevante que os equipamentos tenham baixo consumo de energia e bateria duradoura. Por outro lado, em casos de uso na saúde, controle de trânsito e controle industrial, é de suma importância que haja alta disponibilidade do serviço, alta confiança, segurança e baixa latência, de modo a evitar consequências negativas relacionadas com o funcionamento do serviço.[11]

Apesar de tanta heterogeneidade na construção dos casos de uso da Internet das Coisas, o estabelecimento de padronizações é peça chave para viabilizar a realização de projetos com múltiplos fornecedores. Veremos que não se trata de uma padronização geral para tudo que diga respeito à Internet das Coisas, mas para as várias

9. "Se não tem sensores ou atuadores que lhe permitem características de controle, um objeto está no plano de computação e comunicação, é uma máquina em rede; se não tem capacidade de comunicação, é um sistema de controle digital; se não tem capacidades computacionais, é o que antigamente se chamava [e ainda existem, hoje] sistemas de telemetria. Coisas, aqui pra nós, têm as três características, e todas elas digitais. A gente até poderia dizer que coisas, no sentido de internet das ***coisas***, são *objetos digitais completos*." Grifos no original. MEIRA, Silvio. *Sinais do futuro imediato #1: a internet das coisas.* Disponível em: https://silvio.meira.com/silvio/sinais-do-futuro-imediato-1-internet-das-coisas/. Acesso em: 09/01/2023

10. A ENISA define a Internet das Coisas como *"um ecossistema cyber-físico de sensores e atuadores interconectados, que habilitam tomada de decisão."* Referida Agência ainda destaca que os sensores são "*blocos-chave para a construção da Internet das Coisas, uma vez que são elementos integrais que permitem monitorar o ambiente e o contexto no qual os sistemas de IoT operam".* A definição de atuadores, por sua vez, é feita pela ENISA da seguinte forma: *"uma entidade responsável por mover ou controlar um sistema ou mecanismo. Em termos simples, um atuador opera na direção reversa de um sensor. Toma um* input *elétrico e o transforma em ação."* Tradução livre. European Union Agency for Network and Information Security (ENISA). *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.* pp. 12, 19 e 20. Disponível em: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. Acesso em: 12/12/2022

11. AKPAKWU, Godfrey et al. *A Survey on 5G networks for the Internet of Things Communication: Technologies and challenges.* Disponível em: https://ieeexplore.ieee.org/abstract/document/8141874 . Acesso em: 13/01/2023.

camadas que compõem a sua arquitetura. As telecomunicações são um grande exemplo de estabelecimento de padrões, tendo em vista o seu funcionamento interoperável por definição e a necessidade de prestação de serviços em *roaming*.

Com efeito, a ITU[12] destacou a importância da padronização e da interoperabilidade para a evolução da Internet das Coisas. A criação de padrões é fundamental para que qualquer produto ou serviço seja viável em mais de uma localidade.

A padronização é benéfica em múltiplos aspectos: tanto pela ótica dos fabricantes ou prestadores de serviços, que poderão ter sua tecnologia, seus serviços ou produtos ofertados e vendidos em quaisquer países, dado que serão interoperáveis; como pela ótica dos usuários, que estarão familiarizados com os produtos ou serviços e poderão optar por aqueles que lhes convenham.

A necessidade de padronização é potencializada, na era da computação ubíqua, pela convergência de diferentes plataformas de comunicação e computação. A ITU dá exemplos de padronizações já realizadas, como o acesso à internet por computadores ou celulares, ou ainda a utilização do *bluetooth* pelo computador ou pelo celular. A referida entidade destaca, ainda, a importância das padronizações para o comércio internacional[13]:

A previsão feita em 2005 pela ITU para fins da Internet das Coisas foi de que as padronizações se dariam por meio de protocolos abertos, evoluindo para uma infraestrutura moderna comum, como no caso da energia elétrica e dos motores a vapor[14].

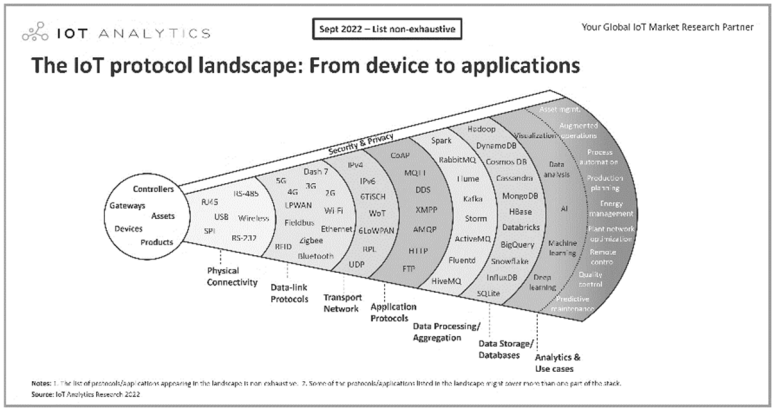
Até agora não se desenvolveu neste sentido, entretanto, o cenário da padronização e interoperabilidade de conexões e dispositivos. Apesar da reconhecida importância dos protocolos, a sua adoção no âmbito da Internet das Coisas não é simples, visto que, como já mencionado, envolve múltiplas camadas que precisam ser

12. *Op. Cit, p. 75*

13. "A definição de padrões é agora parte integral das estratégias de desenvolvimento tecnológico, tanto para atores privados quanto públicos e vai se tornar ainda mais importante em razão da rápida inovação, crescente penetração tecnológica e da importância da tecnologia para o crescimento econômico. O mantra na corrida pelos padrões parece ser: ´se você perder padronizações internacionais, perderá mercados." *Op. Cit., p. 79.* Tradução livre

14. *Op. Cit., p. 78*

compatibilizadas, como ilustra a figura abaixo, numa análise de 2022 da IoT Analytics [15].



É possível ver na imagem acima que os protocolos de comunicação para Internet das Coisas trazem vários padrões e, entre eles, as várias gerações de redes de telecomunicações. A gestão de conectividade por meio de softwares foi apontada, pelo *site* IoT Analytics, como um dos relevantes fatores na adoção de protocolos para a IoT e este é um dos elementos transformadores da conectividade na telefonia celular de quinta geração, conforme será possível ver mais adiante.

Palatella[16] et. al. avaliam os diferentes padrões de conectividade estabelecidos e os comparam entre si, considerando sua aderência com KPIs – *key performance indicators* necessários para a tecnologia de transmissão da Internet das Coisas. A sua conclusão foi colocada na tabela abaixo.

TABLE I
IoT Key Performance Indicators (KPIs) covered by modern connectivity technologies.

	ZigBee	BLE	LP-Wifi	LPWA	3GPP Rel8	LTE Rel13 & NB-IoT
Scalability	✗	✗	✓	✗	✓	✓
Reliability	✗	✓	✓	✗	✓	✓
Low Power	✓	✓	✓	✓	✗	✓
Low Latency	✗	✓	✓	✗	✓	✓
Large Coverage	✗	✗	✓	✓	✓	✓
Low module cost	✓	✓	✓	✓	✗	✓
Mobility support	✗	✗	✗	✗	✓	✓
Roaming support	✗	✗	✗	✗	✓	✓
SLA support	✗	✗	✗	✗	✓	✓

15. PARASKEVOPOULOS, Dimitri. *5 things to know about IoT protocols.* Disponível em: https://iot-analytics.com/iot-protocols/ . Acesso em: 14/11/2022.
16. *Op. cit., p. 16.*

Ao falar sobre as tecnologias em telecomunicações, Palatella *et al*[17] destacam a tendência de que as conexões MTC (ou *Machine-Type Communications*), fundamentais para a conexão na Internet das Coisas, ocorram por meio da tecnologia celular, considerando o fato de que as conexões sem fio permitem maior escalabilidade das soluções e que as redes sem fio são mais baratas do que as redes fixas (considerando que o custo do cobre, assim como mão-de-obra de instalação e manutenção têm se tornado cada vez mais caros)[18].

Dizem ainda os referidos autores que as redes sem fio permitem suportar grande número de dispositivos, com baixo consumo de energia e baixo custo, conectando sensores e dispositivos aos sistemas centrais através de API[19] padronizada, tudo no formato *real-time*, escalável e seguro. As redes de telecomunicações, de fato, têm a vantagem de possuir cobertura global, faturamento, segurança, suporte de qualidade do serviço (QoS), suporte de mobilidade e *roaming,* ecossistema interoperável e a possibilidade de prestar serviços críticos de tráfego[20]. A confiabilidade da operação das referidas redes em âmbito mundial é um fator de grande relevância para a Internet das Coisas.

Para a comunicação MTC, ainda, o 3GPP estabeleceu como requisito que as suas tecnologias sejam todas compatíveis com as *releases* legadas, ou seja, aquelas relacionadas com as gerações anteriores de telefonia celular. Trata-se de elemento de fundamental importância, que permitirá a adequada operação de dispositivos mais antigos, em redes modernas ou mais antigas.

Além da alta confiabilidade das redes de telecomunicações, o 5G, assim como a tecnologia LTE, evolução do 4G, trouxeram novas tecnologias de gestão de rede que serão importantes habilitadores do desenvolvimento e aprimoramento de casos de

17. *Op. Cit.,* p. 5
18. BRAGA, Lucas. *Operadoras denunciam roubo de 4 milhões de metros de cabos de internet.* Disponível em: https://tecnoblog.net/noticias/2022/03/30/operadoras-denunciam-roubo-de-4-milhoes-de-metros-de-cabos-de-internet/ Acesso em: 23/12/2022.
19. FABRO, Clara. *O que é API e para que serve? Cinco perguntas e respostas.* Disponível em: https://www.techtudo.com.br/listas/2020/06/o-que-e-api-e-para-que-serve-cinco-perguntas-e-respostas.ghtml. Acesso em: 12/11/22.
20. *Op. Cit., p. 5*

uso na Internet das Coisas[21]. Abaixo alguns elementos dessas novas funcionalidades, que trazemos apenas para que ilustrem as mudanças possíveis, mas sem adentrar a seara das especificidades técnicas das gerações de telefonia e das *releases* do 3GPP, que pertencem a outra área de especialidade.

(1) Fatiamento de rede (*Network slicing*) – permite que a rede seja implementada e use várias redes "core" para finalidades distintas ("A rede "core" é o coração da rede. Ela estabelece conectividade segura e confiável da rede para usuários finais e dá acesso aos seus serviços").[22] O 3GPP dá exemplos de utilizações de rede em fatias diferentes, como o serviço normal para usuários de uma operadora, os serviços para os usuários de uma rede virtual (conhecida como MVNO[23]), utilização máquina-a-máquina (M2M ou machine-to-machine; ou ainda MTC – *Machine-Type Communication*).

(2) Virtualização de função de rede (*Network Functions Virtualization*) – permite que os operadores de rede gerenciem e façam a expansão das suas capacidades de rede, usando aplicações baseadas em software e, portanto, virtuais, em substituição à infraestrutura física que fazia parte da arquitetura[24]. Significa dizer que os softwares de gerenciamento de rede, em vez de se basear na infraestrutura da operadora, ficarão na nuvem, num fenômeno chamado de "cloudificação" da rede[25]. O diferencial da NFV reside tanto na possibilidade de gerenciar dispositivos heterogêneos de Internet das Coisas, como na escalabilidade e grande flexibilidade em gerenciar e operar dispositivos móveis[26].

---

21. 3GPP. *5G system overview.* Disponível em: https://www.3gpp.org/technologies/5g-system-overview. Acesso em: 27/01/23.
22. Tradução livre. ERICSSON. *5G Core (5GC)* Disponível em: https://www.ericsson.com/en/core-network/5g-core#:~:text=What%20is%205G%20Core%3F,provides%20access%20to%20its%20services. Acesso em: 26/12/2022
23. No Brasil, a atuação como rede virtual, ou Mobile Virtual Network Operator (MVNO), é regulamentada pela Resolução nº 550/2010, da Anatel.
24. ERICSSON. *NFV*. Disponível em: https://www.ericsson.com/en/nfv Acesso em: 26/12/2022
25. EUROPEAN COMMISSION. NIS COOPERATION GROUP. *Report on the Cybersecurity of Open RAN*. Disponível em: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks. Acessado em 02/02/2023
26. *Op. Cit., p. 11*

(3) Computação de borda (*EDGE Computing*) – é a replicação de servidores centrais de uma rede o mais perto possível do usuário final, de maneira a viabilizar certos usos em que o tempo de resposta é crítico, como fábricas do futuro e direção autônoma de veículos.

(4) Rede definida por software *(Software Defined Networking)* - A SDN separa o tráfego dos elementos de redes, como *switches,* roteadores e *hosts* do plano de controle, ou seja, das decisões sobre a rota de tráfego. Isso permite a programação da rede por meio de aplicações externas, simplificando o seu controle. Palatella et al[27] destacam que a arquitetura de rede tradicional não consegue adequadamente gerenciar a quantidade de dispositivos e dados colocados na rede pelos negócios da Internet das Coisas e por isso é tão importante o gerenciamento eficaz do volume de tráfego e dos recursos de redes na era do 5G. Segundo eles, essa flexibilidade de gerenciamento também permite a existência de diferentes requisitos de qualidade de serviço nas redes.

Para que sejam implementadas todas as funcionalidades da quinta geração de telefonia celular, é necessário que a rede tenha arquitetura Stand-Alone (SA), em que todos os componentes da rede 5G são também implementados. Já na arquitetura Non-Stand Alone (NSA), os elementos de acesso 5G (rádio) são conectados ao "core" de uma rede 4G. Nesta modalidade, as funcionalidades de acesso, ou rádio, são aproveitadas, sendo possível usufruir da baixa latência do 5G, mas não de todas as funcionalidades de rede mencionadas acima[28].

Claro que a implantação de projetos NSA é menos onerosa para as operadoras de telecomunicações, uma vez que há o aproveitamento de recursos da rede 4G já implantados. O que vai determinar a utilização da arquitetura SA ou NSA na Internet das Coisas, de todo modo, são os casos de uso.

É crescente a quantidade de projetos em que são demandadas redes privadas de Internet das Coisas e 5G, com requisitos técnicos e de segurança específicos, customizados para segmentos de atuação e necessidades diferentes[29].

---

27. *Op. Cit., p. 11*

28. *Op. Cit.*

29. PRESCOTT, Roberta. *Redes privadas: um filão de ouro para novas receitas com o 5G no Brasil.* Disponível em: https://www.convergenciadigital.com.br/Telecom/Redes-privadas%3A-um-

Desta forma, o 5G, como colocado anteriormente, parece ser o habilitador ótimo das conexões para Internet das Coisas, uma vez que as novas funcionalidades para o gerenciamento de rede permitirão desenhar soluções específicas para cada caso de uso, endereçando os problemas da Internet das Coisas, que estão relacionados com escalabilidade das soluções, heterogeneidade dos dispositivos, interoperabilidade, gerenciamento de tráfego, disponibilidade do serviço e latência, entre outros.

3. 5G E OPEN RAN

O aumento de possibilidades oferecidas pela tecnologia é diretamente proporcional ao aumento da complexidade geral subjacente ao gerenciamento desta tecnologia. Os posicionamentos dos países na criação de padrões de conectividade quanto à adoção de certos produtos ou serviços não devem ser olhados isoladamente, uma vez que suas consequências se espraiam não apenas sobre os negócios e inovação, mas também sobre a segurança, a vigilância e sobre a geopolítica envolvendo os diferentes atores.

O mundo assistiu, por exemplo, às sanções impostas à Huawei pelos Estados Unidos (entre outros países)[30] anos depois que Edward Snowden denunciou a existência de *backdoors* em equipamentos americanos[31]. As discussões em torno da quinta geração de redes de telefonia celular culminaram no banimento da Huawei nos Estados Unidos, nos demais países dos chamados Five Eyes[32] e em alguns países da União Europeia.

---

filao-de-ouro-para-novas-receitas-com-o-5G-no-Brasil-62460.html. Acesso em: 15/02/2023.

30. G1. *5G: entenda a briga entre Estados Unidos e China.* Disponível em: https://g1.globo.com/tecnologia/noticia/2021/11/05/5g-entenda-a-briga-entre-estados-unidos-e-china.ghtml. Acesso em: 22/01/2023.
31. "Um relatório de junho de 2010 do chefe do Departamento de Desenvolvimento de Acesso e Alvos da NSA é de uma clareza chocante. A agência recebe ou intercepta, de forma rotineira, roteadores, servidores e outros equipamentos de rede que serão exportados pelos Estados Unidos antes que sejam despachados para os clientes internacionais. Ela então implanta ferramentas de vigilância do tipo porta dos fundos, reembala os produtos com um selo de fábrica e os despacha. Assim, a NSA consegue acesso a redes inteiras e aos seus usuários." GREENWALD, Glenn. *Sem lugar para se esconder*. Rio de Janeiro: Sextante, 2014. p. 156.
32. Os Five Eyes são Austrália, Canadá, Reino Unido, Nova Zelândia e Estados Unidos.

Em meio às discussões sobre os padrões de operação da rede, surgiu a possibilidade de uma arquitetura aberta, com o Open RAN. Plantin[33] destaca que em 2020, os Estados Unidos determinaram o fomento do desenvolvimento da tecnologia Open RAN, como elemento alternativo à RAN – *Radio Access Network*. Como veremos mais adiante, a União Europeia se posicionou de forma distinta, ao requerer a observância de alguns requisitos na evolução dos padrões, mas sem determinar especificamente aquele que deveria ser buscado.

A RAN, por meio dos seus componentes, conecta os dispositivos dos usuários finais (como os celulares) às redes "core". Isso usualmente acontece por meio dos equipamentos de alguns fabricantes, em um pacote composto por hardware e software combinados, que são implantados na rede de telecomunicações. Planin[34] argumenta que hoje, este mercado é dominado por apenas alguns fornecedores e se trata de uma tecnologia cara, sem grandes incentivos para inovação tecnológica.

Com o Open RAN, haveria a possibilidade de utilizar os recursos da quinta geração de redes de telefonia, a saber, a virtualização do gerenciamento de redes e a desvinculação entre software e hardware (permitindo que um mesmo equipamento contenha softwares distintos para diferentes funções na rede ou que seja utilizada a nuvem para armazenamento de software).

A partir das *features* acima referenciadas, torna-se possível que o gerenciamento dos recursos de RAN aconteça, também, fora do âmbito dos hardwares dos fabricantes tradicionais, na rede das operadoras de telecomunicações. Essa nova tecnologia, em princípio, traria mais flexibilidade e melhores resultados para o gerenciamento de rede, além de estímulo à competição. LIYANAGE destaca que mesmo os *players* menores poderiam implementar suas próprias soluções e a inteligência adicionada ao Open RAN permitiria aumento de automação e performance por meio da

33. Como destacado pelo próprio Plantin, trata-se de conduta similar àquela adotada na China no que diz respeito ao desenvolvimento de tecnologias de quinta geração. PLANTIN, Jean- Christophe. *The geopolitical hijacking of open networking: the case of Open RAN*. Disponível em: https://www.researchgate.net/publication/350875082_The_political_hijacking_of_open_networking_The_case_of_open_radio_access_network. Acesso em: 12/02/2022

34. *Op., cit., p. 406*

otimização do RAN e dos elementos de rede.[35]

PLANTIN[36] destaca que, de um lado, a rede RAN é bastante confiável, tendo em vista que seus fornecedores são conhecidos e fornecem soluções que integram hardware e software. De outro, o fato de que a rede 5G requer uma grande quantidade de antenas diminui a possibilidade de que as operadoras utilizem componentes mais baratos de forma otimizada.

O Open RAN permitiria a abertura das redes de telecomunicações, permitindo a entrada de atores menores e proporcionando, para as operadoras de telecomunicações, o gerenciamento de recursos de forma a que a relação custo-benefício seja mais favorável.

De outro lado, PLANTIN[37] aponta para o risco de não se considerar o Open RAN sob o ponto de vista estratégico, caso não avaliado que em vez de permitir a entrada de novos atores, o Open RAN pode reforçar estruturas dominantes de mercado, adicionando, para as operadoras de telecomunicações, além da dependência dos fornecedores tradicionais de componentes de rede, a dependência de plataformas de tecnologia.

Isso se daria, ainda segundo PLANIN[38], porque:

1 - A abertura que se pretende implementar através do Open RAN não quer dizer que se trate de tecnologia aberta: há abertura em relação à entrada de outros atores, mas cada um com sua tecnologia proprietária;

2 - Os atuais fornecedores de redes de telecomunicações integram os consórcios de discussão de padrões do Open RAN, o que pode significar que investirão na tecnologia específica, sendo prudente atentar para a possibilidade de que se mantenham

35. LIYANAGE, Madhusanka et al. *OPEN RAN Security: Challenges and Opportunities.* Disponível em: https://arxiv.org/abs/2212.01510 . Acesso em: 01/02/2023.

36. O fato curioso é que se trata de conduta similar àquela adotada na China no que diz respeito ao desenvolvimento de tecnologias de quinta geração. PLANTIN, Jean- Christophe. *The geopolitical hijacking of open networking: the case of Open RAN.* Disponível em: https://www.researchgate.net/publication/350875082_The_political_hijacking_of_open_networking_The_case_of_open_radio_access_network. Acessado em 12/02/2022.

37. Ainda na crítica de Plantin, o interesse no Open RAN pelas grandes plataformas de tecnologia vai de encontro ao modelo de plataformas verticais integradas e proprietárias. *Op. Cit.,* p. 411.

38. *Op. Cit., p. 412*

à frente do mercado também neste caso, inclusive em razão de as redes legadas trazerem componentes desses fornecedores;

3 - A "cloudificação" de rede, possível no 5G e no Open RAN, poderia ensejar uma situação em que os atuais provedores de nuvem, alguns poucos com grande domínio de mercado, tenham o controle dessa infraestrutura.

Sobre os consórcios de discussão do Open RAN, a Open Ran Alliance, ou O-RAN[39], criada em 2018, produz um trabalho complementar ao do 3GPP, estabelecendo as especificações relacionadas à tecnologia de rádio: ela separa os elementos do RAN e detalha como eles vão se conectar com demais elementos de rede no modelo Open RAN[40]. Foi formado, em 2020, novo ator para o tema do desenvolvimento de padrões desta tecnologia, que é a Open RAN Policy Coalition, constituída em 2020 por empresas globais[41].

A existência de múltiplas entidades definindo padrões para o Open RAN pode aumentar a complexidade da conectividade para Internet das Coisas, visto que não apenas a rede tem agora vários elementos novos de gerenciamento, como também haverá padrões criados por diferentes entidades. Isso pode inclusive gerar efeitos indesejáveis, como o domínio de alguns fornecedores sobre certas tecnologias, criadas por determinados grupos de padronização.

Com esta preocupação em mente, a Comissão Europeia, por meio do Grupo de Trabalho NIS[42], requereu em maio/22 que as especificações da O-RAN Alliance atendessem aos princípios fundamentais para desenvolvimento de padrões internacionais da Organização Mundial de Comércio, de forma a aumentar a transparência e a abertura da participação de uma quantidade maior de *stakeholders,* possibilitando as avaliações de segurança previstas no Regulamento 1025/2012, que prevê as regras de

39. *"A O-RAN Alliance foi fundada em fevereiro de 2018 pela AT&T, China Mobile, Deutsche Telekom, NTT Dokomo e Orange. Foi constituída como uma entidade alemã."* Tradução livre. O-RAN Alliance. *About us.* Disponível em: https://www.o-ran.org/about#:~:text=About%20us,About%20O%2DRAN%20ALLIANCE,German%20entity%20in%20August%202018. Acesso em: 06/02/2023.

40. *Op. Cit., p. 407 e 409*

41. Open RAN Policy Coalition. *Members*. Disponível em: https://www.openranpolicy.org/about-us/members/. Acesso em: 06/02/2023

42. *Op. Cit., p. 14*

padronização, ou normalização, no âmbito da União Europeia.

A Comissão Europeia chegou inclusive a propor que essas discussões fossem migradas para o 3GPP e propôs, também, que os padrões fossem validados pelo ecossistema, o que inclui empresas de telecomunicações e autoridades, que, em seu entendimento, devem realizar auditorias e devem ter recursos e *expertise* necessários para lidar com esta arquitetura mais complexa[43].

O Grupo de Trabalho acima referenciado apontou para a possibilidade de que o Open RAN ampliasse alguns problemas atuais de rede, como configuração inadequada decorrente da ausência de padrões maduros e da multiplicidade de soluções que podem vir a ser disponibilizadas, além do desenvolvimento de produtos de baixa qualidade.

Ainda segundo a Comissão Europeia, o Open RAN também cria riscos novos, tais como problemas de segurança que levam ao aumento da superfície de ataques cibernéticos, ausência de controles suficientes para certas funções de rede que estejam virtualizadas e maior complexidade para resolução de problemas de rede (dada a dificuldade de identificar causa raiz e realizar a resolução, num cenário com múltiplos provedores de solução).[44]

Como toda tecnologia em envolvimento e evolução, o Open RAN dá mostras de que passará por muito debate e proporcionará relevantes transformações no desenvolvimento de produtos e serviços voltados à conectividade da rede 5G e das futuras gerações de redes de telecomunicações. Permanece importante a análise estratégica dos interesses dos diferentes atores e as consequências para os modelos de produtos, serviços, segurança e tratamentos de dados relacionados.

4. SEGURANÇA E PRIVACIDADE DOS USUÁRIOS NO 5G E NA INTERNET DAS COISAS

A quinta geração de telefonia celular, além de trazer os elementos de segurança da terceira e quarta gerações (criptografia da interface aérea, ainda muito relacionada com os serviços de voz, e mecanismo robusto de autenticação dos usuários), trouxe

43. *Op. Cit., p. 10*

44. *Op. Cit., pp. 7 a 9*

outros aprimoramentos, tais como algoritmos de criptografia em estado-da-arte, sistemas mais elaborados de gerenciamento de chaves de acesso, proteção da integridade do sinal e autenticação mútua entre a rede e o dispositivo[45].

Apesar de o 5G trazer as melhorias de segurança identificadas acima, outros elementos adicionam complexidade: o Open RAN, como vimos, por aumentar a quantidade de empresas atuando na rede de telecomunicações, aumenta a necessidade de verificações de segurança e controle de acesso e, por este motivo, oferece maior superfície de ataques cibernéticos.

A isso se deve somar o fato de que as coisas conectadas à Internet das Coisas, ou Objetos Digitais Completos, por vezes, são produtos pequenos ou não concebidos originalmente para a conectividade, que não comportam a inserção de códigos ou mecanismos de segurança ou de autenticação o que gera vulnerabilidades e acaba sendo um importante vetor de ataques cibernéticos.[46] [47] Esses ataques não apenas podem ferir a privacidade dos usuários, como podem se tornar vetores de invasões a outras infraestruturas, como no caso de utilização de dispositivos como "bots" para ataques de negação de serviço (o "DDoS Attack")[48].

A privacidade dos usuários também deve ser objeto de preocupação. A ENISA[49] aponta que a Internet das Coisas muda drasticamente a forma como os dados são coletados, analisados, utilizados e protegidos. MAGRANI[50] relaciona 4 grandes riscos à privacidade, gerados pela Internet das Coisas, a saber:

> (1) a identificação do titular de dados, associando sua identidade a quantidades massivas de dados; segundo o autor, decorre não apenas da quantidade de dispositivos

45. *Op. Cit., p. 7*
46. TOULAS, Bill. *Researchers warn of severe risks from ´Printjack´ printer attacks. Disponível em:* https://www.bleepingcomputer.com/news/security/researchers-warn-of-severe-risks-from-printjack-printer-attacks/. Acesso em: 09/02/2023.
47. BELLA, Giampaolo et al. *Multi-service threats: Attacking and protecting network printers and VoIP phones alike.* Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S2542660522000130?via%3Dihub. Acesso em: 15/01/2023.
48. IBM. *The weaponization of IoT devices: Rise of the thingbots.* Disponível em: https://www.ibm.com/downloads/cas/6MLEALKV. Acesso em: 13/12/2022.
49. *Op. Cit.,* P. 7
50. *Op. cit., p. 96*

que coletam impressões digitais, biometria e outros dados dos usuários, mas também da ilusão da anonimização (entendimento de que há irreversibilidade de associação, quando na verdade, não há, em razão de técnicas inadequadas de anonimização);

(2) o rastreamento do titular, pelo fato de que as redes que estabelecem a conectividade dos usuários na Internet das Coisas muitas vezes coletam a sua localização, sendo que frequentemente ele sequer sabe que seus dados estão sendo coletados. No modelo de conectividade Open RAN, como já mencionado anteriormente, dada a possibilidade de aumento na quantidade de empresas fazendo parte da arquitetura de rede e considerando ainda a dificuldade de gerenciamento de acessos que é pertinente a um modelo com vários *players*, pode haver ainda um desvio de informações de localização sem controle adequado;

(3) o *profiling* ou perfilamento, considerando que a Internet das Coisas, conforme já dito mais acima, trata dados pessoais de um modo jamais visto. São coletados dados pessoas os mais diversos, com atributos pouco usuais (decorrentes da utilização dos dispositivos), em altíssimo volume, que são usados na busca de *insights* de negócios, dentro do fenômeno do Big Data.[51].

(4) a disponibilização indevida de dados do usuário caso, no processo de alteração do ciclo de vida do dispositivo, como por exemplo, troca ou venda do produto para um terceiro, dados do titular disponibilizados a terceiro. A construção dos dispositivos ou das funcionalidades de modo a permitir a autenticação do titular, portanto, permanece um desafio.

A preservação da privacidade do usuário, bem como as medidas a serem tomadas no âmbito da Internet das Coisas, decorrerão de uma miríade de interações entre fabricantes de Objetos Digitais Completos, de componentes de redes e de tecnologias de conectividade, que precisarão ser extensivamente discutidos com todos os *players*, seja para fins de definição de padronizações, seja para a discussão dos casos de uso específico em que possam ser mitigadas vulnerabilidades e assegurados os tratamentos de dados pessoais dentro dos parâmetros normativos existentes.

51. MENDES, Laura Schertel et al. *Discriminação algorítmica à luz da Lei Geral de Proteção de Dados.* In: Tratado de Proteção de Dados Pessoais. Coord.: Laura Schertel Mendes et al. Rio de Janeiro: Forense, 2021., p. 424

5. CONCLUSÃO

O potencial da Internet das Coisas vem sendo comemorado como elemento determinante para mudar a o comportamento dos indivíduos na vida em rede. Os seus benefícios, como vimos, já eram previstos ainda na época da terceira geração de telefonia celular, tendo em vista o que acabava de ser conquistado por meio da conectividade ao alcance da mão.

O 5G, por sua vez, vem trazer uma mudança que vai muito além do aumento na velocidade da transmissão de dados ou na quantidade de dispositivos simultaneamente conectados. Ao analisar as possibilidades que são oferecidas pelos novos parâmetros de gerenciamento de rede da quinta geração de telefonia celular, é possível perceber que está sendo operada uma transformação profunda na forma como diversos *stakeholders* vão atuar no ecossistema da Internet das Coisas.

Os novos casos de uso e a forma como cada fornecedor de produto ou serviço, ou operadora de telefonia celular poderão atuar ainda não são amplamente conhecidos, sendo possível que surjam novos *players* para soluções inovadoras.

Se, de um lado, as perspectivas do uso da rede 5G para a Internet das Coisas são as melhores possíveis, de outro, não se deve descuidar da análise estratégica a respeito da influência que exercem os governos e empresas privadas na determinação dos padrões de operação, assim como não se pode perder de vista o exercício sobre as consequências das mudanças que já começaram a acontecer.

REFERÊNCIAS

3GPP. *5G system overview.* Disponível em: https://www.3gpp.org/technologies/5g-system-overview. Acesso em: 02/12/22.

3GPP. *Introducing 3GPP*. Disponível em: https://www.3gpp.org/ftp/Information/presentations/3GPP_PowerPoint_template . Acesso em: 12/01/23.

3GPP. *Partnership Project Description.* Disponível em: https://www.3gpp.org/images/downloads/partnership-project-description.pdf. Acesso em: 12/01/2023.

AKPAKWU, Godfrey et al. *A Survey on 5G networks for the Internet of Things Communication: Technologies and challenges.* Disponível em: https://ieeexplore.ieee.org/abstract/document/8141874 . Acesso em: 13/01/2023.

BRAGA, Lucas. *Operadoras denunciam roubo de 4 milhões de metros de cabos de internet*. Disponível

em: https://tecnoblog.net/noticias/2022/03/30/operadoras-denunciam-roubo-de-4-milhoes-de-metros-de-cabos-de-internet/ Acesso em: 23/12/2022.

BELLA, Giampaolo et al. *Multi-service threats: Attacking and protecting network printers and VoIP phones alike.* Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S2542660522000130?via%3Dihub. Acesso em: 15/01/2023.

CHAGAS, Everton. *IoT: Criação de Produtos nas Operadoras de Telecomunicações no Brasil.* Disponível em: http://bibliotecadigital.fgv.br/ocs/index.php/ctd/ctd2019/paper/viewFile/7329/2108 . Acessado em: 22/02/2023.

ERICSSON. *5G Core (5GC)* Disponível em: https://www.ericsson.com/en/core-network/5g-core#:~:text=What%20is%205G%20Core%3F,provides%20access%20to%20its%20services. Acesso em: 26/12/2022.

ERICSSON. *NFV*. Disponível em: https://www.ericsson.com/en/nfv Acesso em: 26/12/2022.

EUROPEAN COMMISSION. NIS COOPERATION GROUP. *Report on the Cybersecurity of Open RAN.* Disponível em: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks. Acesso em 02/02/2023.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. Disponível em: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. Acesso em: 12/12/2022.

FABRO, Clara. *O que é API e para que serve? Cinco perguntas e respostas.* Disponível em: https://www.techtudo.com.br/listas/2020/06/o-que-e-api-e-para-que-serve-cinco-perguntas-e-respostas.ghtml. Acesso em: 12/11/22.

G1. *5G: entenda a briga entre Estados Unidos e China.* Disponível em: https://g1.globo.com/tecnologia/noticia/2021/11/05/5g-entenda-a-briga-entre-estados-unidos-e-china.ghtml. Acesso em: 22/01/2023.

GREENWALD, Glenn. *Sem lugar para se esconder*. Rio de Janeiro: Sextante, 2014.

IBM. *The weaponization of IoT devices: Rise of the thingbots*. Disponível em: https://www.ibm.com/downloads/cas/6MLEALKV. Acesso em: 13/12/2022.

ITU – International Telecommunication Union. The Internet of Things. Geneva, 2005. (ITU Internet Reports 2005). Disponível em: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf. Acesso em: 08/12/2022.

LIYANAGE, Madhusanka et al. *OPEN RAN Security: Challenges and Opportunities.* Disponível em: https://arxiv.org/abs/2212.01510 . Acesso em: 01/02/2023.

MENDES, Laura Schertel et al. *Discriminação algorítmica à luz da Lei Geral de Proteção de Dados.* In: Tratado de Proteção de Dados Pessoais. Coord.: Laura Schertel Mendes et al. Rio de Janeiro: Forense, 2021.

O-RAN Alliance. *About us.* Disponível em: https://www.o-ran.org/about#:~:text=About%20us,About%20O%2DRAN%20ALLIANCE,German%20entity%20in%20August%202018. Acesso em: 06/02/2023.

Open RAN Policy Coalition. *Members*. Disponível em: https://www.openranpolicy.org/about-us/members/. Acesso em: 06/02/2023.

PRESCOTT, Roberta. *Redes privadas: um filão de ouro para novas receitas com o 5G no Brasil.* Disponível em: https://www.convergenciadigital.com.br/Telecom/Redes-privadas%3A-um-filao-de-ouro-para-novas-receitas-com-o-5G-no-Brasil-62460.html. Acesso em: 15/02/2023.

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

MEIRA, Silvio. *23 anotações sobre 2023 [x] - 5G & Internet das Coisas*. Disponível em: https://silvio.meira.com/silvio/23-anotacoes-sobre-2023-x/ Acesso em: 09/01/2023.

MEIRA, Silvio. *Sinais do futuro imediato #1: a internet das coisas.* Disponível em: https://silvio.meira.com/silvio/sinais-do-futuro-imediato-1-internet-das-coisas/. Acesso em: 09/01/2023.

PALATELLA, Maria Rita et. al. *Internet of Things in the 5G Era: Enablers, Architecture and Business Models*. Disponível em: https://orbilu.uni.lu/bitstream/10993/24796/1/main_jsac.pdf Acesso em: 22/02/2023.

PARASKEVOPOULOS, Dimitri. *5 things to know about IoT protocols.* Disponível em: https://iot-analytics.com/iot-protocols/ . Acesso em: 14/11/2022.

PLANTIN, Jean- Christophe. *The geopolitical hijacking of open networking: the case of Open RAN.* Disponível em: https://www.researchgate.net/publication/350875082_The_political_hijacking_of_open_networking_The_case_of_open_radio_access_network. Acesso em: 12/02/2022.

TAPARIA, Anand. *IoT 2022 in Review: The 10 Most Relevant IoT Developments of the Year.* Disponível em: https://iot-analytics.com/iot-2022-in-review/. Acesso em: 31/01/2023.

TOULAS, Bill. *Researchers warn of severe risks from ´Printjack´ printer attacks. Disponível em:* https://www.bleepingcomputer.com/news/security/researchers-warn-of-severe-risks-from-printjack-printer-attacks/. Acesso em: 09/02/2023.

V
NOVOS CONTEXTOS DE APLICAÇÃO

HERANÇA DIGITAL NO BRASIL: DESAFIOS JURÍDICOS E PERSPECTIVAS

Natália Cristina Chaves

Doutora em Direito pela Universidade Federal de Minas Gerais. Professora de Direito Empresarial da Faculdade de Direito da UFMG. Sócia fundadora da Passos e Chaves Sociedade de Advogados.

DOI: https://doi.org/10.59224/dti5.ch15

Resumo: Neste estudo, analisam-se os desafios jurídicos da herança digital no Brasil. O primeiro desafio diz respeito à transmissibilidade do acervo digital. Doutrina e jurisprudência divergem sobre a temática. A pluralidade de projetos legislativos contrapostos evidencia a necessidade de aprofundamento do debate. Diante disso, o planejamento sucessório revela-se como ferramenta apta a reduzir a insegurança jurídica em caso de falecimento do titular de acervo digital. Ao final, ver-se-á que não há respostas prontas para os problemas apresentados, sendo indispensável uma maior reflexão sobre o tema.

Palavras-chave: Herança; digital; falecimento.

Abstract: *In this study, the legal challenges of digital heritage in Brazil are analyzed. The first challenge concerns the transmissibility of the digital asset. Doctrine and jurisprudence diverge on the subject. The plurality of opposing legislative projects highlights the need to deepen the debate. In front of this, succession planning proves to be a tool capable of reducing legal uncertainty in the event of the death of the owner of a digital asset. In the end, it will be seen that there are no ready answers to the problems presented, being indispensable a deepening of the reflections on the theme.*

Keywords: *Inheritance; digital; death.*

1. INTRODUÇÃO

Com a inauguração da chamada Era Digital, marcada pela dinamização do fluxo de informações no ambiente virtual, vive-se um novo ciclo na história da humanidade. O acesso da população à internet, intensificado no final do século XX,

propiciou a difusão do conhecimento, bem como o compartilhamento de ideias e pensamentos em escala jamais experimentada, abarcando pessoas das mais diversas localidades, num movimento de integração mundial e de ressignificação da forma de se relacionar.

Diante desse contexto de revolução comunicacional e de avanços tecnológicos, as relações jurídicas se transformam, colocando à prova o ordenamento jurídico existente. Se, até então, o Direito revelou-se satisfatório à regulação da vida em sociedade, o que se traduz na máxima *ubi societas, ibi jus*, aproxima-se o momento de se repensar o sistema jurídico como um todo ou ele submergirá em meio a esse processo de mudanças.

No campo do Direito das Sucessões, o movimento já se faz sentir, seja pela maior complexidade das relações familiares, seja pelo fenômeno da globalização, que impulsionou as sucessões transnacionais.

Mas, não é só. Com as inovações proporcionadas pela tecnologia, o Direito das Sucessões enfrenta, agora, o desafio trazido por uma nova categoria de bens imateriais, a saber, os bens digitais.

Segundo Laura Marques Gonçalves, os bens digitais "(...) *se relacionam aos elementos contidos no ambiente virtual, criados em sistema de linguagem binária, que requerem algum dispositivo eletrônico para serem acessados e que dialogam com o universo incorpóreo, imaterial e intangível*"[1].

Em síntese, os bens digitais são bens imateriais armazenados virtualmente, tais como criptomoedas, milhas aéreas, ativos em jogos *on line*, canais de YouTube, entre outros exemplos.

Muito se discute acerca da transmissibilidade dos bens digitais na hipótese de falecimento de seu titular, já que, nem sempre, referidos bens cumprem uma função meramente econômica. É precisamente diante desse contexto que os bens digitais podem oferecer a maior dificuldade sob a perspectiva do Direito Sucessório no Brasil.

1. GONÇALVES, Laura Marques. *Transmissão* post mortem *de patrimônio digital:* em defesa da ampla sucessão. Dissertação apresentada ao Programa de Pós-Graduação da Faculdade de Direito da Universidade Federal de Minas Gerais, 2021. Disponível em: https://repositorio.ufmg.br/handle/1843/41742. Acesso em: 22 fev. 2023. p. 31.

Com efeito, admitir a sua transmissibilidade naqueles casos em que os bens digitais têm um cunho existencial, refletindo aspectos da vida privada de seu titular, ainda que tal perfil seja conjugado com um conteúdo econômico, pode significar a violação a direitos da personalidade, tanto do titular desses bens quanto de terceiros, os quais são resguardados constitucionalmente[2].

A questão se torna ainda mais complexa face à omissão do ordenamento jurídico brasileiro, quanto a essa herança digital. Não obstante a tramitação, no Congresso Nacional, de alguns projetos de lei acerca da matéria, ainda hoje, subsiste a lacuna, ficando a cargo do Judiciário a difícil tarefa de dar a solução mais adequada a cada caso concreto, a partir das normas em vigor.

De modo a suprir essa lacuna legislativa identificada não apenas no Brasil, mas, também, no exterior, as plataformas digitais têm buscado, em seus termos de uso, direcionar o caminho a ser trilhado na hipótese de falecimento de seus usuários, oferecendo a possibilidade de tais usuários, previamente, determinar o destino de sua conta em caso de morte. Contudo, tais regulamentos são passíveis de questionamento e têm alcance limitado.

Para além desses regulamentos, o próprio titular dos bens digitais sobre os quais pairam a dúvida da transmissibilidade poderá deixar, em vida, a sua manifestação de vontade acerca da destinação de tais bens, hipótese em que sua vontade deverá ser respeitada, observados os parâmetros legais.

Uma vez fixados os contornos dos bens digitais passíveis de transmissão *causa mortis*, constituindo a chamada herança digital, ainda há desafios adicionais, ligados à avaliação desses bens e à consequente tributação em caso de morte.

Na sequência, abordar-se-ão os principais desafios relativos à herança digital e apontar-se-ão as perspectivas para o seu tratamento no Brasil.

2. O art. 5º, inciso X, da Constituição brasileira dispõe que: "*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...]*". (BRASIL. *Constituição da República Federativa do Brasil de 1988, de 5 de outubro de 1988*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 fev. 2023).

2. O DEBATE DOUTRINÁRIO ACERCA DA TRANSMISSIBILIDADE DOS BENS DIGITAIS

Analisando-se os bens digitais, verifica-se que podem ter um cunho patrimonial, existencial ou dúplice[3].

Os bens digitais de cunho patrimonial[4] são aqueles que cumprem "*função econômica, passível de conversão em pecúnia, tendo por objeto interesses financeiros e por escopo o lucro*"[5]. Podem ou não pressupor a apropriação e, em caso positivo, são transmissíveis *causa mortis*, compondo a chamada herança digital[6].

---

3. Nesse sentido, KONDER, Nelson; TEIXEIRA, Ana Carolina Brochardo. O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 51. *E-book*.
4. Sobre o acervo digital de valor econômico, por sua vez, Marco Aurélio de Farias Costa Filho esclarece: "*Considerando seu evidente potencial econômico, o acervo digital deve ser considerado na sucessão patrimonial. A aferição de seu valor pode inclusive afetar a legítima destinada aos herdeiros e a parte disponível para ser legada pelo autor da herança. Bens virtuais raros, arquivos armazenados virtualmente potencialmente valiosos para efeitos de propriedade intelectual e até sites ou contas que podem servir como fonte de renda após a morte de seu titular são apenas alguns exemplos de formas de patrimônio que, ainda que não sejam mencionadas em testamento, não devem ser ignoradas pela partilha. Caso contrário, haverá claro prejuízo aos direitos dos herdeiros*". (COSTA FILHO, Marco Aurélio de Farias. *Patrimônio digital:* reconhecimento e herança. Recife: Nossa Livraria, 2016. p. 148).
5. KONDER, Nelson; TEIXEIRA, Ana Carolina Brochardo. O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 52. *E-book*.
6. Consoante Clóvis Beviláqua, o Direito das Sucessões é o "*complexo dos princípios, segundo os quais se realiza a transmissão do patrimônio de alguém, que deixa de existi*r", sendo, portanto, a herança, o patrimônio transmitido pelo *de cujus*. (BEVILÁQUA, Clóvis. *Direito das sucessões.* 5. ed. rev. e atual. Rio de Janeiro: Francisco Alves, 1955. p. 11). Segundo Camila Helena Melchior Baptista de Oliveira e Gustavo Tepedino, "*o direito de herança se constitui tradicionalmente como corolário do direito de propriedade (art. 5º, XXII e XXIII, CF/88), de modo que a sucessão* causa mortis *tem por objeto exclusivamente a transferência de situações jurídicas de cunho patrimonial. Vale dizer: o objeto da sucessão, em última análise, consiste em bens e direitos suscetíveis de avaliação pecuniária e que, como tal, integram o patrimônio do* de cujus. *Partindo-se de tal premissa, compreende-se que a herança digital, decorrente do direito fundamental à herança previsto no art. 5º, XXX, da Constituição Federal, consiste na universalidade de bens digitais e direitos de cunho patrimonial,*

Ao lado dos bens digitais com valor econômico, há aqueles de cunho existencial, os quais refletem aspectos da vida privada do seu titular. São ligados à personalidade de seu titular, possuindo valor afetivo. Sendo desprovidos de expressão econômica, essa subcategoria de bens digitais, na qual se inserem, por exemplo, arquivos de fotos digitais e e-mails do indivíduo, está, a princípio, excluída da herança digital, não se transmitindo aos sucessores.

Isso porque, de acordo com o art. 11 do Código Civil, excetuados os casos previstos em lei, "*os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária*"[7].

Na confluência das duas subcategorias de bens digitais abordadas, emerge uma terceira subcategoria, em que os bens digitais são marcados por uma dúplice função, a saber, econômica e existencial[8].

Se, quanto à subcategoria dos bens digitais de cunho patrimonial não restam dúvidas quanto à sua transmissibilidade aos herdeiros em caso de falecimento de seu

---

transmissíveis aos herdeiros, por sucessão causa mortis". (OLIVEIRA, Camila Helena Melchior Baptista de; TEPEDINO, Gustavo. *Streaming* e herança digital. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 132-133. *E-book*).

7. Segundo Paulo Lôbo, "*o CC anterior aludia aos bens 'fora do comércio', a saber, os que não podem ser objeto de disposição ou negociação, quando um interesse maior se apresenta. Os direitos da personalidade ou as zonas ambientais protegidas são exemplos de bens que não podem ser transmitidos de seu titular para outrem. Quando o direito exclui um bem do tráfico jurídico – ou o põe 'fora do comércio'-, determina sua natureza de uso pessoal, de uso comunitário e até mesmo de não uso, no atendimento a valores relevantes*". (LÔBO, Paulo. *Direito civil:* parte geral. 5. Ed. São Paulo: Saraiva, 2015. p. 191).
8. Conforme destaca Fernando Taveira Jr., "*As contas de redes sociais, que armazenam fotografias digitais e mensagens, de cunho extrapatrimonial, ao mesmo tempo, podem conter valores econômicos, já que, por meio destas contas, é possível realizar transações comerciais ou financeiras, por links, em sítios externos (livraria, de compra coletiva etc.). Ou seja, a pessoa conectada à conta de sua rede social pode realizar compras em outras webpages especializadas. O melhor exemplo deste tipo de transação é proporcionado pela ferramenta Facebook Connect, disponível aos usuários do Facebook.*" (TAVEIRA JR., Fernando. *Bens digitais (digital assets) e a sua proteção pelos direitos da personalidade:* um estudo sob a perspectiva da dogmática civil brasileira. Porto Alegre: Revolução eBooks – Simplíssimo, 2018. p. 64).

titular, quanto às demais subcategorias, divergem os doutrinadores[9].

De um lado, há aqueles que, pautados no princípio da *saisine* e da sucessão universal, entendem pela transmissibilidade de todo o acervo de bens do *de cujus*, incluindo os bens digitais sem conteúdo econômico ou com função híbrida (econômica e existencial)[10].

Referida corrente doutrinária ganhou força a partir de 2018, com o emblemático desfecho de uma disputa judicial na Alemanha, envolvendo o *Facebook*, em que a mais alta corte alemã, o *Der Bundesgerichtshof* (BGH), decidiu pela transmissibilidade da herança digital aos pais, herdeiros legítimos de uma adolescente que faleceu, tragicamente, em decorrência de um acidente em metrô[11].

Em síntese, dita adolescente possuía uma conta na plataforma digital *Facebook*, sendo que, com o seu falecimento e a subsequente comunicação, por um terceiro, de aludido evento, tal conta foi convertida em memorial, de modo que seus pais perderam o acesso ao conteúdo privado dela, apesar de que tinham a posse do *login* e senha pessoais de sua filha.

Visando a obter maiores detalhes sobre as circunstâncias da morte de sua filha, não só em virtude da suspeita de suicídio, mas também da necessidade de se obterem elementos de defesa em face de uma ação indenizatória ajuizada pelo condutor do

9. Sobre as duas correntes doutrinárias predominantes acerca do tema, ver: HONORATO, Gabriel; LEAL, Lívia Teixeira. Exploração econômica de perfis de pessoas falecidas: reflexões jurídicas a partir do caso Gugu Liberato. *In: Revista brasileira de direito civil*. Belo Horizonte, v. 23, p. 163-164, jan./mar. 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/523/350. Acesso em: 25 fev. 2023.

10. O art. 1.784 do Código Civil dispõe que: "*Aberta a sucessão, a herança transmite-se, desde logo, aos herdeiros legítimos e testamentários*". (BRASIL. Lei n. 10.406, de 10 de jan. de 2002. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 25 fev. 2023). Nesse sentido, ver: GONÇALVES, Laura Marques. *Transmissão* post mortem *de patrimônio digital:* em defesa da ampla sucessão. Dissertação apresentada ao Programa de Pós-Graduação da Faculdade de Direito da Universidade Federal de Minas Gerais, 2021. Disponível em: https://repositorio.ufmg.br/handle/1843/41742. Acesso em: 22 fev. 2023.

11. Sobre o aludido caso, consultar: ADOLFO, Luiz Gonzaga Silva; KLEIN, Júlia Schroeder Bald. Herança digital: diretrizes a partir do *leading case* do Der Bundesgerichtshof. *In: Revista brasileira de direito civil*. Belo Horizonte, v. 30, p. 183-199, out./dez. 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/687/502. Acesso em: 25 fev. 2023.

metrô envolvido no fatídico acidente, os pais da adolescente requereram, ao *Facebook*, o acesso à rede social da filha, o que foi negado. A justificativa dada pelo *Facebook* foi embasada na proteção à privacidade, tanto da falecida quanto de terceiros que com ela se comunicaram por meio da plataforma.

Diante da referida negativa, os pais da adolescente ingressaram com ação judicial objetivando o acesso ao conteúdo privado da conta de sua filha. Em primeira instância, o pedido foi acolhido, ao passo que, em segunda instância, o Tribunal de Apelação na Alemanha reverteu a decisão, prestigiando a tutela do direito à privacidade. Em última instância, a decisão foi novamente revisada, tendo, a Corte alemã, ancorada no princípio da sucessão universal, reconhecido o direito dos pais da adolescente, enquanto seus legítimos herdeiros, à herança digital, com acesso à sua rede social no *Facebook*.[12].

Além de ter afastado o argumento de que o acesso à rede social da adolescente implicaria violação aos direitos da personalidade dela e/ou de terceiros, a Corte alemã também afastou a concepção de que somente os bens digitais com conteúdo econômico seriam transmissíveis, adotando a tese de que a transmissibilidade abarcaria tanto o acervo digital de cunho patrimonial quanto aquele de cunho

12. Referido caso foi detalhadamente narrado por Luiz Gonzaga Silva Adolfo e Júlia Schroeder Bald Klein, nos seguintes termos: "[...] *o* leading case *afastou o argumento de que o reconhecimento do direito sucessório à herança digital afrontaria os direitos da personalidade do* de cujus *e dos terceiros interlocutores. Conforme o BGH, o sigilo das comunicações no* Facebook *é assegurado somente para impedir que pessoas estranhas tenham acesso ao conteúdo do perfil. Para os magistrados, os herdeiros, por força legal do seu direito sucessório, não podem ser enquadrados como desconhecidos na relação jurídica. Nessa conjuntura, assemelharam o armazenamento de dados em plataforma digital aos documentos em papel, os quais, embora guardados em gavetas fechadas, podem ter sua confidencialidade rompida a qualquer momento. As regras e os princípios do direito das sucessões permitem a plena e automática transmissão do patrimônio digital e analógico aos herdeiros legítimos do falecido, salvo disposição diversa em contrário. Para o* Der Bundesgerichtshof, *não há que se alegar qualquer ofensa ao direito de personalidade* post mortem *do autor da herança ou dos terceiros interlocutores, ainda que seja um consectário da inviolabilidade da dignidade da pessoa humana, consagrado no art. 1º, inc. I, da Lei Fundamental alemã (*Das Grundgesetz – *GG*)". (ADOLFO, Luiz Gonzaga Silva; KLEIN, Júlia Schroeder Bald. Herança digital: diretrizes a partir do *leading case* do *Der Bundesgerichtshof*. *In: Revista brasileira de direito civil*. Belo Horizonte, v. 30, p. 190, out./dez. 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/687/502. Acesso em: 25 fev. 2023).

existencial.[13].

No Brasil, aqueles que se colocam favoráveis à ampla transmissibilidade dos bens digitais, seguindo o princípio da sucessão universal, são minoria, sendo que a doutrina prevalente é no sentido de que alguns bens digitais não seriam transmissíveis, sobretudo quando impliquem violação aos direitos da personalidade da pessoa que falece e de terceiros. Consoante referida corrente, à qual também se adere, como regra, somente se transferem os bens que desempenhem função patrimonial, não se transmitindo conteúdos que contenham aspectos personalíssimos e existenciais que remetam à vida privada da pessoa que falece e de terceiros[14].

Contudo, mesmo no tocante aos bens digitais com caráter exclusivamente existencial, a intransmissibilidade deve ser mitigada à luz do princípio da dignidade da

13. "*[...] o Tribunal alemão descartou a tese de que os herdeiros legítimos somente poderiam suceder bens de caráter econômico. No entendimento da Corte, a legislação sucessória não faz distinção entre a herança com valor monetário e a herança com valor estritamente sentimental. Diários e cartas sempre foram transmitidos aos herdeiros com a morte do seu titular, embora contivessem informações confidenciais. Logo, seria incoerente permitir o acesso a conteúdo físico e materialmente palpável e proibir a obtenção de informações armazenadas em plataformas digitais. Se o intuito da distinção do conteúdo de cada bem digital seria o de proteção da personalidade do autor da herança, mormente sua privacidade e intimidade, essa tutela deveria ser realizada em qualquer meio, seja no ambiente digital, seja no analógico. O caráter existencial não se alterna a depender da forma como o objeto está corporificado. A extrapatrimonialidade é verificada pelo teor do bem, seja ele consubstanciado no meio cibernético ou não. Portanto, para o BGH, não haveria razão axiológica para adotar entendimentos distintos para bens virtuais e para bens analógicos, ao passo que ambos apresentam vieses econômicos, como também sentimentais*". (ADOLFO, Luiz Gonzaga Silva; KLEIN, Júlia Schroeder Bald. Herança digital: diretrizes a partir do *leading case* do *Der Bundesgerichtshof. In: Revista brasileira de direito civil.* Belo Horizonte, v. 30, p. 191, out./dez. 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/687/502. Acesso em: 25 fev. 2023).

14. De acordo com Paulo Lôbo, "*o que se transmite não é o direito da personalidade, mas a projeção de seus efeitos patrimoniais, quando haja. O direito permanece inviolável e intransmissível, ainda que o titular queira transmiti-lo, pois o que é inerente à pessoa não pode ser dela destacado. A pessoa não transmite sua imagem, ficando dela privada durante certo tempo, o que acarretaria sua despersonalização. O que se utiliza é certa e determinada projeção de sua imagem (a foto, o filme, a gravação), que desta se originou*". (LÔBO, Paulo. *Direito civil:* parte geral. 5. Ed. São Paulo: Saraiva, 2015. p. 132).

pessoa humana, que tem como um dos substratos, a liberdade[15]. A propósito, o próprio indivíduo, previamente ao seu falecimento, pode manifestar a sua vontade no sentido da transmissão de todo o seu acervo digital aos seus sucessores, hipótese em que a sua vontade deveria prevalecer[16].

Discussões ainda maiores envolvem aqueles bens com dupla função, tanto existencial quanto patrimonial, tais como perfis em redes sociais e canais no *YouTube*, em que uma dada pessoa pode inserir os dados pessoais para fins financeiros, monetizando aspectos de sua vida privada. É o caso, por exemplo, de influenciadores digitais, blogueiros e outras celebridades, cujas postagens publicizam, no ambiente virtual, a privacidade desses profissionais, para fins econômicos. Aqui, o público e o privado se mesclam, não sendo possível identificar onde começa um e onde termina o outro.

Daí porque, nessas situações, a análise acerca da transmissibilidade ou não do acervo digital com dúplice função deve levar em consideração o destino que seria

15. Segundo Ana Luiza Nevares, "*uma releitura do Direito Civil torna-se imperiosa, sendo certo que, no campo da sucessão legítima, deve-se buscar uma real e concreta proteção ao sucessor, a partir de suas especificidades e características, à luz de suas relações com o falecido e com os bens integrantes da herança. De outro moo, o Direito Sucessório torna-se um espaço vazio para a promoção da dignidade da pessoa humana, tendo um papel exclusivamente patrimonial*". (NEVARES, Ana Luiza. *A sucessão do cônjuge e do companheiro na perspectiva do direito civil constitucional.* 2. ed. São Paulo: Atlas, 2015. p. 141).

16. Como elucidam Ana Carolina Brochardo Teixeira e Nelson Konder: "*Esta intangibilidade absoluta dos direitos da personalidade por ato de vontade é cotidianamente desmascarada pela realidade social, ao ponto de se buscar em doutrina mitigações ao dispositivo legal. Alega-se, em restrição ao texto do dispositivo legal, que em verdade somente seria vedada a renúncia definitiva, a disposição permanente, permitindo-se atos temporários ou limitados de cessão de atributos vinculados à personalidade. Melhor caminho trilha a doutrina que reconhece relativa a necessidade de interpretar o dispositivo à luz da garantia constitucional de liberdade, vinculada à própria dignidade humana. Neste sentido, uma vez que a autonomia para escolher como realizar mais adequadamente sua personalidade faz parte da própria tutela da personalidade, qualquer forma de limitação ou restrição absoluta ao poder de disposição configuraria ato de paternalismo incompatível com pluralismo democrático que rege a ordem constitucional*". (KONDER, Nelson; TEIXEIRA, Ana Carolina Brochardo. O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 54-55. *E-book*).

mais adequado à tutela da personalidade do seu titular, sopesando a sua autonomia existencial e, portanto, os atos de disposição relativamente à projeção de efeitos de sua personalidade praticados em vida e a não mercantilização da pessoa humana[17].

Disso se infere que não há uma resposta pronta para a questão da transmissibilidade ou intransmissibilidade do acervo digital, quando este abarcar aspectos da vida privada de seu titular, sendo que o endereçamento desse acervo deverá ser decidido casuisticamente, levando em consideração a melhor forma de realização da personalidade daquele que faleceu, à luz da dignidade da pessoa humana.

Observa-se, portanto, que a solução para a celeuma jurídica que se instalou reveste-se, atualmente, de elevada carga de subjetividade, demandando o sopesamento de princípios, o que conduz a decisões judiciais conflitantes.

3. A JURISPRUDÊNCIA BRASILEIRA ACERCA DA (IN)TRANSMISSIBILIDADE DO ACERVO DIGITAL

A jurisprudência acerca da temática da transmissibilidade de herança digital ainda é tímida no Brasil. O primeiro caso de que se tem notícia remonta a 2013, na Cidade de Campo Grande, no Mato Grosso do Sul, quando a mãe de uma falecida jovem ingressou com uma ação contra o Facebook Serviços Online do Brasil Ltda. (processo n. 0001007-27.2013.8.12.0110), após as infrutíferas tentativas de solucionar a questão administrativamente, para cancelar o perfil da filha na plataforma. Tal

17. A esse respeito, pertinentes são os ensinamentos de Ana Carolina Brochardo Teixeira e Nelson Konder: "*Reconhecendo-se a possibilidade* a priori *de atos de disposição de atributos da própria personalidade como forma de realização pessoal, coloca-se o dilema de como,* a posteriori*, evitar eventuais desvios que possam importar em mercantilização ou instrumentalização da pessoa humana. Essas situações jurídicas dúplices constituídas a partir do exercício da autonomia negocial sobre bens da personalidade são ilustrativas desta dificuldade. Com efeito, a análise funcional não se presta a avaliar a transmissibilidade, comunicabilidade e renunciabilidade em abstrato, mas destina-se ao controle de merecimento de tutela, em concreto, de cada ato de exercício das situações jurídicas subjetivas*". (KONDER, Nelson; TEIXEIRA, Ana Carolina Brochardo. O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 57. *E-book*).

perfil havia sido convertido em memorial, gerando sofrimento para a família[18].

Em 2017, na Cidade de Pompeu, em Minas Gerais, uma mãe ingressou com ação judicial em face da *Apple Computer Brasil Ltda.*, objetivando a senha de acesso ao *iCloud* da filha falecida. Como a filha não havia deixado, em vida, permissão para esse acesso a seus sucessores, o pedido foi negado, em 08/06/2018, com fundamento na proteção à privacidade, não tendo ocorrido a interposição de recurso[19].

Em 2019, uma mãe ingressou com ação de obrigação de fazer, conjugada com indenização por danos morais em face do Facebook Serviços Online do Brasil Ltda., em virtude de a plataforma ter excluído o perfil de sua filha, após ciência de seu falecimento. Como alegado pela mãe, ela passou a usar o perfil de sua filha falecida, com o objetivo de recordar fatos da vida desta última, bem como de interagir com pessoas próximas. Isso se revelava possível na medida em que a mãe tinha acesso ao usuário e à senha da filha. Em primeira instância, os pedidos formulados pela genitora foram julgados improcedentes. Em segunda instância, o Tribunal de Justiça de São Paulo manteve o referido entendimento, já que a filha da autora/apelante teria aderido aos termos de uso do *Facebook*, os quais preveem as hipóteses de destinação da conta na aludida plataforma, após o falecimento do usuário, não se revelando possível o restabelecimento de dita conta. De acordo com o voto do i. Desembargador Relator, a

18. Consoante tutela de urgência deferida nos autos do referido processo: "*O perigo na demora está consubstanciado no direito da personalidade, tanto da pessoa morta quanto da mãe (art. 12, parágrafo único, do CC), sanando o sofrimento decorrente da transformação do perfil em "muro de lamentações", o que ataca diretamente o direito à dignidade da pessoa humana da genitora, que além do enorme sofrimento decorrente da perda prematura de sua única filha, ainda tem que conviver com pessoas que cultivam a morte e o sofrimento. Se não bastasse, os comentários poderão até se transformarem em ofensas à personalidade da pessoa já falecida, pois estão disponíveis livremente aos usuários do* Facebook*. Assim, a autora possui legitimidade para pleitear o bem da vida consistente na exclusão do perfil de sua falecida filha do* Facebook*, razão pela qual o pedido liminar deve ser acolhido*". (BRASIL. Tribunal de Justiça do Mato Grosso do Sul. Processo n. 0001007-27.2013.8.12.0110. 1ª Vara do Juizado Especial Central de Campo Grande. Juíza Vânia de Paula Arantes. Julgado em 19 mar. 2013. Disponível em: https://www.migalhas.com.br/arquivo_artigo/art20130424-11.pdf. Acesso em: 26 fev. 2023).

19. BRASIL. Tribunal de Justiça do Estado de Minas Gerais. Processo n. 0023375-92.2017.8.13.0520. Vara Única da Comarca de Pompeu. Juiz Manoel Jorge de Matos Júnior. Julgado em 08 jun. 2018. Disponível em: https://www.tjgm.jus.br. Acesso em: 26 fev. 2023.

disputa "*deve ser dirimida à luz de dispositivos constitucionais e civilistas, gizada notadamente pelos direitos da personalidade e pelo princípio da autonomia da vontade, o que leva ao respeito da manifestação de vontade exarada pela titular da conta*", em especial a sua adesão aos Termos de Serviço do *Facebook*[20]. Ainda de acordo com tal voto, "*o pungente e veloz crescimento do número de usuários da internet e de seus recursos trouxe implicações jurídicas que resvalam em indagações a respeito da possibilidade ou não de transmissão do acesso às suas contas pessoais em redes sociais aos eventuais herdeiros*"[21]. Como o caso envolve situação jurídica existencial na rede, prevalece "*a lógica de proteção assentada nos direitos da personalidade, como a privacidade e a identidade, que são direitos pessoais e intransmissíveis*"[22].

Em outro caso originário da Comarca de Itapecerica da Serra, em São Paulo, uma filha menor e herdeira única, representada por sua genitora, ingressou, em 2017, com ação judicial contra a Apple Computer Brasil S/A, visando ao acesso de dados armazenados na nuvem, correspondente à conta *Apple* do celular de seu falecido pai. Segundo a autora, o pedido de acesso permitiria não só a recuperação de fotografias e demais dados do *de cujus,* mas, também, poderia auxiliar na investigação criminal relativa ao falecimento do *de cujus,* vítima de latrocínio. A ação foi julgada procedente em primeira instância e o Tribunal de Justiça paulista, em julgamento realizado em março de 2021, manteve o posicionamento[23].

---

20. BRASIL. Tribunal de Justiça do Estado de São Paulo. 31ª Câmara Cível de Direito Privado. Apelação Cível n. 1119688-66.2019.8.26.0100. Relator Des. Francisco Casconi. Julgado em 09 mar. 2021. Disponível em: www.tjsp.jus.br. Acesso em: 27 fev. 2023.
21. BRASIL. Tribunal de Justiça do Estado de São Paulo. 31ª Câmara Cível de Direito Privado. Apelação Cível n. 1119688-66.2019.8.26.0100. Relator Des. Francisco Casconi. Julgado em 09 mar. 2021. Disponível em: www.tjsp.jus.br. Acesso em: 27 fev. 2023.
22. BRASIL. Tribunal de Justiça do Estado de São Paulo. 31ª Câmara Cível de Direito Privado. Apelação Cível n. 1119688-66.2019.8.26.0100. Relator Des. Francisco Casconi. Julgado em 09 mar. 2021. Disponível em: www.tjsp.jus.br. Acesso em: 27 fev. 2023.
23. Segundo o voto do i. Desembargador Relator, Rômulo Russo: "*Com efeito, os autos tratam do direito de acessibilidade à memória digital; fotografias e mensagens atreladas à vida familiar do titular morto, que podem ser acessadas por sua única herdeira. A memória digital é equivalente àquela que se encontra fora do aparelho celular. Verte direito substantivo à proteção da memória daquele, cuja titularidade alcança o cônjuge, os ascendentes ou os descendentes (art. 20, § único, do Cód. Civil). Conquanto não se trate de pleito que se dirija à proteção dos predicados da pessoa*

Mais recentemente, em janeiro de 2022, o Tribunal de Justiça mineiro, em julgamento de agravo de instrumento, manteve a decisão agravada, no sentido de indeferir o pedido da agravante de quebra de sigilo das contas e dispositivos *Apple* do *de cujus*. Conforme sustentado no voto da i. Desembargadora Relatora, acompanhado pelos demais julgadores, "*os direitos da personalidade são intransmissíveis, permanecendo invioláveis mesmo após a morte de seu titular* [...]"[24]. Seguindo esse raciocínio, seria transmissível apenas a projeção dos efeitos patrimoniais dos direitos da personalidade, o que não restaria presente no caso analisado.

Como se vê, os julgados acerca da matéria são incipientes, oscilando entre a transmissibilidade e a intransmissibilidade do acervo digital, tendendo para a última opção naqueles casos em que dito acervo tem cunho existencial, envolvendo aspectos da vida privada do usuário falecido, de modo a prestigiar a tutela aos direitos da personalidade.

4. OS PROJETOS LEGISLATIVOS SOBRE A MATÉRIA

O Código Civil brasileiro não traz regramento específico sobre a herança digital.

De igual modo, a Lei n. 12.965/2014, que inaugurou o Marco Civil da Internet, também não regula a transmissibilidade de acervos digitais, em caso de morte do seu titular, limitando-se a reafirmar a tutela aos direitos da personalidade. Nesse sentido, em seu art. 7º, incisos I a III, são assegurados, aos usuários da *internet*, a inviolabilidade da intimidade e da vida privada, a inviolabilidade e sigilo do fluxo de comunicações na *internet* e das comunicações privadas armazenadas, ressalvadas as hipóteses de autorização judicial[25]. Seguindo essa linha, no art. 10 do mencionado Diploma

falecida, a memória imaterial é útil apenas à sua única herdeira; do contrário, sem nexo com a vida mantê-la incólume. Pode dizer-se que é direito que decorre da interpretação sistemática do art. 1.788 do Cód. Civil". (BRASIL. Tribunal de Justiça do Estado de São Paulo. 7ª Câmara Cível de Direito Privado. Apelação Cível n. 100433442.2017.8.23.0268. Relator Des. Rômulo Russo. Julgado em 31 mar. 2021. Disponível em: www.tjsp.jus.br. Acesso em: 27 fev. 2023).

24. BRASIL. Tribunal de Justiça do Estado de Minas Gerais. 3ª Câmara Cível. Agravo de Instrumento n. 1.0000.21.190675-5/001. Relatora Des. Albergaria Costa. Julgado em 27 jan. 2022. Disponível em: www.tjmg.jus.br. Acesso em: 27 fev. 2023.

25. O art. 7º da Lei n. 12.965/2014 assim preceitua: "*O acesso à* internet *é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da*

legal, estabelece-se que a guarda e a disponibilização de registros de conexão, de dados pessoais e de conteúdo de comunicações privadas devem resguardar a intimidade, a vida privada, a honra e a imagem das pessoas envolvidas direta ou indiretamente. Sob essa perspectiva, o provedor responsável pela guarda somente estará obrigado a disponibilizar tais informações por ordem judicial, respeitando-se os direitos da personalidade[26].

Mais recentemente, a Lei Geral de Proteção de Dados (Lei n. 13.709/2018) passou a regular o tratamento de dados pessoais, inclusive nos meios digitais, visando à "*proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*"[27]. Entre os seus fundamentos, o art. 2º de aludida Lei assegura o respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem, reafirmando a proteção aos direitos da personalidade. A preocupação com a preservação da intimidade e da privacidade permeia diversos dispositivos da Lei Geral de Proteção de Dados[28], muito embora se tenha perdido a oportunidade de tratar, especificamente, da transmissibilidade de dados pessoais na

---

vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...]". (BRASIL. *Lei n. 12.965/2014, de 23 de abril de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 fev. 2023).

26. O art. 10 da Lei n. 12.965/2014 dispõe que: "*A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de* internet *de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. §1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no* caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. [...]*".
27. Art. 1º da Lei Geral de Proteção de Dados. BRASIL. *Lei n. 13.907, de 14 de agosto de 2018*. Lei geral de proteção de dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 fev. 2023.
28. A título exemplificativo, cita-se o art. 17 de mencionado Diploma, o qual preceitua que: "*Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei*".

hipótese do falecimento de seu titular.

Diante desse quadro de omissão legislativa, ao longo dos últimos anos, foram propostos diversos Projetos de Lei acerca da matéria.

O primeiro deles a surgir foi o de n. 4.099, de 2012, de iniciativa do então Deputado Federal Jorginho Mello, arquivado em 2019. Tal Projeto propunha a inserção de um parágrafo único ao art. 1.788 do Código Civil, no sentido da transmissibilidade de todo o acervo digital[29].

O segundo Projeto, de n. 4.847, também do mesmo ano, foi de autoria do Deputado Federal Marçal Filho e propunha o acréscimo de 3 (três) dispositivos ao Código Civil, a saber, os arts. 1.797-A, 1.797-B e 1.797-C[30]. No primeiro deles, cuidou-se do conceito de herança digital, enquanto "*o conteúdo intangível do falecido, tudo o que é possível guardar ou acumular em espaço virtual*", ou seja, senhas, redes sociais, contas da *internet* e qualquer bem e serviço virtual e digital de titularidade do *de cujus*[31]. Já o art. 1.797-B dispunha que, na ausência de testamento, a herança seria transmitida aos herdeiros legítimos. Por fim, o art. 1.797-C atribuía ao herdeiro definir o destino das contas do falecido, transformando-as em memorial, apagando todos os dados do usuário ou removendo a conta do antigo usuário. Esse segundo Projeto também foi arquivado.

Tanto o primeiro quanto o segundo Projetos foram alvo de críticas, sobretudo por tratarem, indistintamente, do acervo digital como um todo, sem uma maior

29. A redação proposta pelo Projeto, para o parágrafo único do art. 1.788 do Código Civil, era a seguinte: "*Serão transmitidos aos herdeiros todos os conteúdos de contas ou arquivos digitais de titularidade do autor da herança*". (BRASIL. Câmara dos Deputados. *Projeto de Lei n. 4.099, de 2012*. Altera o art. 1.788 da Lei n. 10.406, de 10 de janeiro de 2002, que 'institui o Código Civil'. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1004679&filename=Tramitacao-PL%204099/2012. Acesso em: 27 fev. 2023).

30. BRASIL. Câmara dos Deputados. *Projeto de Lei n. 4.847, de 2012*. Acrescenta o Capítulo II-A e os arts. 1.797-A a 1.797-C à Lei n. 10.406, de 10 de janeiro de 2002. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1049733&filename=Tramitacao-PL%204847/2012. Acesso em: 27 fev. 2023.

31. A proposta de redação do art. 1.797-A era a seguinte: "*A herança digital defere-se como o conteúdo intangível do falecido, tudo o que é possível guardar ou acumular em espaço virtual, nas condições seguintes: I - senhas; II - redes sociais; III - contas da Internet; IV - qualquer bem e serviço virtual e digital de titularidade do falecido*".

preocupação com os direitos da personalidade[32].

Novos Projetos sobre herança digital se seguiram nos idos de 2015 e 2017, tendo sido também arquivados[33].

Em 2019, foram apresentados 2 (dois) Projetos de interesse ao tema aqui tratado, os quais ainda se encontram em tramitação, no Congresso Nacional. O primeiro deles, de n. 5.820, é de autoria do Deputado Federal Elias Vaz e é voltado para a alteração do art. 1.881 do Código Civil, incluindo 5 (cinco) parágrafos, entre os quais o parágrafo quarto, que trata da possibilidade de se destinar a herança digital por meio de codicilo em vídeo, com a dispensa de testemunhas[34]. Tal Projeto sofreu ajustes posteriores e, em fevereiro de 2022, foi encaminhado ao Senado Federal, para apreciação. Entre os ajustes realizados, cita-se a nova redação sugerida para o art. 1.876 do Código Civil, a qual introduziu o testamento em vídeo e, ainda, definiu a herança digital como aquela "*constituída de vídeos, fotos, senhas de redes sociais, e-mails e outros elementos armazenados exclusivamente na rede mundial de computadores ou em nuvem*"[35].

32. Acerca da análise dos Projetos, destaca-se o Parecer de autoria de Pablo Malheiros da Cunha Frota, designado pela Comissão de Direito Civil do Instituto dos Advogados Brasileiros, em 12/12/2017. Disponível em: https://www.iabnacional.org.br/pareceres/pareceres-votados/016-2017. Acesso em: 27 fev. 2023.
33. Nesse sentido, citam-se os Projetos de Lei n. 1.331/2015, 7.742/2017 e 8.562/2017.
34. De acordo com o aludido Projeto, na sua versão original, a redação do art. 1.881 do Código Civil passaria a ser a seguinte: "*Art. 1.881. Toda pessoa capaz de testar poderá, mediante instrumento particular, fazer disposições especiais sobre o seu enterro, bem como destinar até 10% (dez por cento) de seu patrimônio, observado no momento da abertura da sucessão, a certas e determinadas ou indeterminadas pessoas, assim como legar móveis, imóveis, roupas, joias entre outros bens corpóreos e incorpóreos. [...] §4º. Para a herança digital, entendendo-se essa como vídeos, fotos, livros, senhas de redes sociais, e outros elementos armazenados exclusivamente na rede mundial de computadores, em nuvem, o codicilo em vídeo dispensa a presença das testemunhas para sua validade. [...]*". (BRASIL. Câmara dos Deputados. *Projeto de Lei n. 5.820, de 2019*. Dá nova redação ao art. 1.881 da Lei no 10.406, de 2002, que institui o Código Civil. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1829027&filename=Tramitacao-PL%205820/2019. Acesso em: 27 fev. 2023).
35. A redação proposta para o art. 1.867 do Código Civil, nos moldes do Projeto de Lei n. 5.820, na versão encaminhada ao Senado Federal, em fevereiro de 2022, é a seguinte: "*Art. 1.867. [...] §3º. [...] II - para a herança digital, constituída de vídeos, fotos, senhas de redes sociais, e-mails e outros*

Já o segundo Projeto, de n. 6.468, é de autoria do Senador Jorginho Mello, e reaviva, no Senado Federal, o antigo Projeto de sua autoria, já arquivado, em que propunha o acréscimo de um parágrafo único ao art. 1.788 do Código Civil, no sentido da transmissão, aos herdeiros, de "*todos os conteúdos de contas ou arquivos digitais de titularidade do autor da herança*", atraindo, novamente, as críticas já feitas no passado[36]. Até a data de elaboração deste artigo, tal Projeto encontrava-se aguardando designação de relator no Senado Federal.

Em 02 de junho de 2020, o Deputado Federal Gilberto Abramo apresentou 2 (dois) Projetos de Lei, a saber, o de n. 3.050 e o de n. 3.051.

No primeiro deles, é proposto o acréscimo de um parágrafo único ao art. 1.788 do Código Civil, admitindo-se a transmissibilidade do acervo digital de cunho patrimonial[37].

O segundo deles, por sua vez, o qual foi apensado ao primeiro, é voltado para o acréscimo do art. 10-A à Lei n. 12.965/2014, de modo a regular a exclusão de contas de usuários mortos por provedores de aplicações de *internet*, mediante o requerimento de cônjuge, companheiro ou parentes até segundo grau[38]. A proposta é de

---

elementos armazenados exclusivamente na rede mundial de computadores ou em nuvem, o testamento em vídeo não dispensa a presença das testemunhas para sua validade; [...]".

36. BRASIL. Senado Federal. *Projeto de Lei n. 6.468, de 2019.* Altera o art. 1.788 da Lei n. 10.406, de 10 de janeiro de 2002, que institui o Código Civil, para dispor sobre a sucessão dos bens e contas digitais do autor da herança. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8056437&ts=1674176579296&disposition=inline. Acesso em: 27 fev. 2023.

37. A redação proposta, no citado Projeto de Lei, para o parágrafo único do art. 1.788 do Código Civil é a seguinte: "*Serão transmitidos aos herdeiros todos os conteúdos de qualidade patrimonial contas ou arquivos digitais de titularidade do autor da herança*". (BRASIL. Câmara dos Deputados. *Projeto de Lei n. 3.050, de 2020.* Altera o art. 1.788 da Lei n. 10.406, de 10 de janeiro de 2002. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1899763. Acesso em: 27 fev. 2023).

38. No Projeto de Lei aqui tratado, propõe-se a redação a seguir para o art. 10-A do Marco Civil da Internet: "*Os provedores de aplicações de* internet *devem excluir as respectivas contas de usuários brasileiros mortos imediatamente, se for requerido por familiares após a comprovação do óbito. §1º A exclusão dependerá de requerimento aos provedores de aplicações de* internet*, em formulário próprio, do cônjuge, companheiro ou parente, maior de idade, obedecida a linha sucessória, reta ou colateral, até o segundo grau inclusive. [...] §3º As contas em aplicações de internet poderão ser mantidas mesmo após a comprovação do óbito do seu titular, sempre que essa opção for*

permitir, também, a manutenção das contas em aplicações de *internet*, mesmo após o óbito do usuário, desde que admitida tal manutenção pelo provedor e haja o requerimento cônjuge, companheiro ou parentes até segundo grau. Um ponto negativo desse segundo Projeto é vincular a manutenção das contas em aplicações de *internet* à permissão do provedor, conferindo maior poder ainda às *big techs* e retirando a autonomia do usuário de dispor dos próprios dados, dando, a seus bens digitais, a destinação que lhe aprouver[39].

Em 2021, foi apresentado novo Projeto de Lei, de n. 1.144, de autoria da Deputada Federal Renata Abreu, de acordo com o qual se propõe a transmissibilidade do acervo digital de cunho econômico e a intransmissibilidade do "*conteúdo de mensagens privadas constantes de quaisquer espécies de aplicações de Internet, exceto se utilizadas com finalidade exclusivamente econômica*"[40].

---

possibilitada pelo respectivo provedor e caso o cônjuge, companheiro ou parente do morto indicados no caput deste artigo formule requerimento nesse sentido, no prazo de um ano a partir do óbito, devendo ser bloqueado o seu gerenciamento por qualquer pessoa, exceto se o usuário morto tiver deixado autorização expressa indicando quem deva gerenciá-la". (BRASIL. Câmara dos Deputados. *Projeto de Lei n. 3.051, de 2020.* Acrescenta o art. 10-A à Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), a fim de dispor sobre a destinação das contas de aplicações de internet após a morte de seu titular. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1899766&filename=Tramitacao-PL%203051/2020. Acesso em: 27 fev. 2023).

39. A esse respeito, destacam-se os ensinamentos de Fernanda Mathias de Souza Garcia: "*A era digital transformou a forma de criação e armazenamento de informações pessoais. Caso prevaleçam as tendências atuais de negativa de transmissão destas com o advento morte, boa parte dos ativos digitais passarão a ser gerenciados inadequadamente por empresas que estão se autorregulando como bem entendem. É claro que tal postura não visa à proteção da privacidade dos usuários, mas sim evitar litígios, reduzir gastos e responsabilidades*". (GARCIA, Fernanda Mathias de Souza. *Herança digital:* o direito brasileiro e a experiência estrangeira. 2. ed. Rio de Janeiro: Lumen Juris, 2022. p. 122. *E-book*).

40. No referido Projeto, introduz-se, no Código Civil, o art. 1.791-A, com a redação a seguir: "*Art. 1.791-A. Integram a herança os conteúdos e dados pessoais inseridos em aplicação da Internet de natureza econômica. §1º Além de dados financeiros, os conteúdos e dados de que trata o* caput *abrangem, salvo manifestação do autor da herança em sentido contrário, perfis de redes sociais utilizados para fins econômicos, como os de divulgação de atividade científica, literária, artística ou empresária, desde que a transmissão seja compatível com os termos do contrato. [...] §3º Não se transmite aos herdeiros o conteúdo de mensagens privadas constantes de quaisquer espécies de*

Como esclarecido na justificativa, "*em se tratando de aspectos da personalidade do indivíduo, parece precipitado pensar sua disciplina jurídica exclusivamente a partir da estrutura do direito sucessório, que está voltado predominantemente à transferência de patrimônio*"[41]. Conforme salientado, "*os direitos de personalidade são intransmissíveis, o que indica a necessidade de uma abordagem diferente em relação ao tema. Embora seja comum falar-se em herança digital, o ideal é que essa ideia se restrinja a aspectos patrimoniais*"[42].

Além disso, o Projeto introduz o art. 10-A ao Marco Civil da Internet, de modo a prever, como regra, a obrigação de os provedores de aplicações de *internet* excluírem as contas públicas de usuários brasileiros mortos, ressalvadas as hipóteses em que: (i) houver previsão contratual em sentido contrário e manifestação do titular dos dados pela sua manutenção após a morte; (ii) os conteúdos e dados pessoais inseridos em aplicação da *Internet* tenham conteúdo econômico, desde que a transmissão seja

aplicações de Internet, exceto se utilizadas com finalidade exclusivamente econômica". (BRASIL. Câmara dos Deputados. *Projeto de Lei n. 1.144, de 2021.* Dispõe sobre os dados pessoais inseridos na internet após a morte do usuário. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1982888&filename=Tramitacao-PL%201144/2021. Acesso em: 27 fev. 2023).

41. ABREU, Renata. *Projeto de Lei n. 1.144, de 2021.* Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1982888&filename=Tramitacao-PL%201144/2021. Acesso em: 27 fev. 2023. p.3-4. Ao delimitar, como regra, a transmissibilidade do acervo digital às hipóteses em que ele tenha conteúdo econômico, a Deputada em comento pautou-se nos ensinamentos de Lívia Teixeira Leal: "*Pode-se verificar que a temática inegavelmente tem sido desenvolvida sob a ótica patrimonial, estando vinculada com frequência a expressões como 'herança digital', 'legado digital', 'patrimônio digital', 'ativo digital', que revelam, em última análise, um exame inicial estritamente patrimonial. [...] Não se pode ignorar que alguns direitos são personalíssimos, e, portanto, intransmissíveis, extinguindo-se com a morte do titular, não sendo objeto de sucessão e não integrando o acervo sucessório por ele deixado. Assim, como a herança refere-se ao acervo patrimonial do* de cujus*, as situações existenciais, ressalvadas as situações dúplices em alguns aspectos, não vão integrar o conceito de herança*". (LEAL, Livia Teixeira. *Internet e morte do usuário:* propostas para o tratamento jurídico *post mortem* do conteúdo inserido na rede. Rio de Janeiro: LMJ Mundo Jurídico, 2018. p. 38).

42. ABREU, Renata. *Projeto de Lei n. 1.144, de 2021.* Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1982888&filename=Tramitacao-PL%201144/2021. Acesso em: 27 fev. 2023. p. 3-4.

compatível com os termos do contrato com o provedor[43]. Novamente, aqui, ressalta-se a preocupação com o poder dado às plataformas digitais.

Aspecto interessante do mencionado Projeto é a previsão de que não só o cônjuge, o companheiro ou o parente em linha reta ou colateral até o quarto grau têm legitimidade para a defesa de ameaça ou lesão aos direitos da personalidade de pessoa falecida, mas também, qualquer pessoa com legítimo interesse, ampliando o rol daqueles que podem agir na tutela de aspectos dos direitos da personalidade de pessoa falecida[44].

Após a apresentação do referido Projeto, que foi apensado ao Projeto n. 3.050, já se seguiram outros Projetos, tais como o de n. 2.664/2021, de autoria do Deputado Federal Carlos Henrique Gaguim. O aludido Projeto também se encontra apensado ao Projeto n. 3.050 e, contrariamente à proposta da Deputada Federal Renata Abreu, acrescenta o art. 1.857-A ao Código Civil, para admitir a transmissibilidade do acervo digital como um todo, sem distinção. Ademais, dito Projeto ainda prevê a nulidade das cláusulas contratuais voltadas para restringir os poderes de uma pessoa para dispor dos próprios dados[45]. Na mesma linha, o Projeto n. 703/2022, de autoria do

43. A redação proposta, no aludido Projeto, para o art. 10-A do Marco Civil da Internet é a seguinte: "*Os provedores de aplicações de* internet *devem excluir as contas públicas de usuários brasileiros mortos, mediante comprovação do óbito, exceto se: I - houver previsão contratual em sentido contrário e manifestação do titular dos dados pela sua manutenção após a morte; II - na hipótese do §1º do art. 1.791-A da Lei n. 10.406, de 10 de janeiro de 2002 (Código Civil). [...]*". (BRASIL. Câmara dos Deputados. *Projeto de Lei n. 1.144, de 2021*. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1982888&filename=Tramitacao-PL%201144/2021. Acesso em: 27 fev. 2023).

44. Nesse sentido, o Projeto sugere a seguinte redação para o parágrafo único do art. 12 do Código Civil: "*Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge ou o companheiro sobrevivente, parente em linha reta, ou colateral até o quarto grau, ou qualquer pessoa com legítimo interesse*". (BRASIL. Câmara dos Deputados. *Projeto de Lei n. 1.144, de 2021*. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1982888&filename=Tramitacao-PL%201144/2021. Acesso em: 27 fev. 2023).

45. BRASIL. Câmara dos Deputados. *Projeto de Lei n. 2.664, de 2021.* Acrescenta o art. 1857-A à Lei n. 10.406, de 2002, Código Civil, de modo a dispor sobre a herança digital. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2049837&filename=PL%202664/2021. Acesso em: 27 fev. 2023.

Deputado Federal Hélio Lopes[46].

Como se vê, a questão é controvertida, sendo que há Projetos em trâmite no Congresso Nacional tanto a favor da transmissibilidade de todo o acervo digital, quanto no sentido de se restringir referida transmissibilidade às situações jurídicas dotadas de valor econômico, o que requer um aprofundamento das discussões em torno do tema.

5. PLANEJAMENTO SUCESSÓRIO DO ACERVO DIGITAL E O DESAFIO DE SUA AVALIAÇÃO

Diante da celeuma que se instaurou no Brasil, no tocante à transmissibilidade ou não do acervo digital a sucessores, na hipótese de falecimento de seu titular, o caminho mais seguro a trilhar é o da prévia manifestação de vontade do usuário acerca da destinação de aludido acervo.

Nesse sentido, nos termos do art. 1.857 do Código Civil, o testamento revela-se como uma alternativa interessante ao titular de bens digitais, tanto de cunho patrimonial quanto existencial, permitindo-lhe que, em vida, determine a destinação desses bens[47]. E tal ato de disposição de vontade em vida, embora tenha as suas limitações, poderá, inclusive, obstar comportamentos lesivos por parte de herdeiros que visem exclusivamente aos fins econômicos. Com efeito, o testamento poderá evitar que a exploração do acervo digital contrarie a verdadeira intenção de seu titular falecido, protegendo os legítimos interesses jurídicos decorrentes dos direitos de personalidade deste último[48].

---

46. BRASIL. Câmara dos Deputados. *Projeto de Lei n. 703, de 2022.* Acrescenta o art. 1857-A à Lei n. 10.406, de 2002, Código Civil. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2152405&filename=PL%20703/2022. Acesso em: 27 fev. 2023.

47. Tal dispositivo legal assim preceitua: "*Toda pessoa capaz pode dispor, por testamento, da totalidade dos seus bens, ou de parte deles, para depois de sua morte. §1º. A legítima dos herdeiros necessários não poderá ser incluída no testamento. §2º. São válidas as disposições testamentárias de caráter não patrimonial, ainda que o testador somente a elas se tenha limitado*".

48. A esse respeito, vale destacar os ensinamentos de Flaviana Rampazzo Soares e Ísis Boll de Araújo Bastos: "*Há limites naturais, por parte do titular, para essa atuação preventiva restritiva das pretensões autorizadoras de futuros sucessores, em razão da perda de força efetiva de ação pós-morte,*

Não há dúvidas, portanto, de que o testamento, observadas as formalidades legais, pode servir de instrumento de proteção da vontade do titular do acervo digital após o seu falecimento, possibilitando, ainda, o resguardo de aspectos dos direitos de personalidade que transcendem a vida do indivíduo, projetando-se *post mortem*. Além disso, o testamento tem a vantagem de poder ser alterado a qualquer tempo, permitindo ajustes ao longo da vida do indivíduo[49].

Sob essa perspectiva, por meio de testamento, o testador pode não só dar a destinação aos bens digitais de valor econômico, mas pode, também, vedar o acesso às suas redes sociais, bem como aos conteúdos inseridos em determinada plataforma digital, sendo que o respeito à sua autonomia privada, enquanto uma das facetas de realização da dignidade da pessoa humana, ao nosso ver, é a solução mais apropriada.

Ao lado do testamento, o codicilo também pode ser um caminho a seguir, contemplando disposições não só sobre bens digitais de cunho patrimonial (desde que de pouca monta), mas também sobre conteúdos de caráter personalíssimo inseridos nas plataformas digitais[50]. Contudo, na prática, pelas suas limitações legais, o codicilo

---

mas a manifestação prévia e escrita de vontade para reduzir o espectro de atuação daqueles que tornaram-se "guardiões" de tais direitos é instrumento adequado a frear pretensões egoístas e distanciadas das legítimas intenções de seu titular, que pode consignar em que termos o uso de seus atributos de personalidade pode se dar. Essa necessidade se torna ainda mais premente naqueles casos em que a imagem, a voz e o nome estão cercados de interesse pela notoriedade, pois tais direitos se revestem de importância a quem deseja preservar qualidades humanas positivas inerentes (inatas ou formadas com o tempo) que constituem sua honra e que, muitas vezes, foram compostas no decorrer da vida e que correm o risco de serem trocadas por dinheiro, sem maiores cautelas. Sabe-se que eventual ambição dos sucessores, aliada a uma natural ânsia curiosa do espectador, pode se tornar uma equação cujo resultado tende a ser perverso à pessoa falecida. Nesses casos, os direitos de personalidade se manifestam com feição econômica indireta patente, e há justo interesse de que eles não sejam objeto de ingerência indevida por parte de herdeiros ou legatários e que não sejam maculadas por interesses meramente egoístas, ilegítimos ou distanciados da vontade da pessoa falecida". (SOARES, Flaviana Rampazzo; BASTOS, Ísis Boll de Araujo. *Avanços tecnológicos e proteção* post mortem *dos direitos de personalidade por meio do testamento*. Revista Fórum de Direito Civil – RFDC. Belo Horizonte, ano 4, n. 10, set./dez. 2015. p. 198).

49. O art. 1.858 do Código Civil estabelece o seguinte: "*O testamento é ato personalíssimo, podendo ser mudado a qualquer tempo*".

50. O art. 1.881 do Código Civil dispõe: "*Toda pessoa capaz de testar poderá, mediante escrito particular seu, datado e assinado, fazer disposições especiais sobre o seu enterro, sobre esmolas de pouca*

perde a relevância para o testamento.

Como se não bastasse, já existem provedores de armazenamento de dados em nuvens que oferecem serviços que propiciam a transferência de bens digitais. O *SecureSafe*, por exemplo, é um provedor de armazenamento de dados que permite manter todos os documentos digitais relevantes e senhas de acesso em um local digital centralizado. Com isso, na eventualidade de falecimento ou de incapacidade do usuário, uma vez ativado um código entregue a alguém de sua confiança, é impulsionado o procedimento para a transferência dos dados ao beneficiário ou beneficiários indicados[51].

Paralelamente às ferramentas mencionadas, as próprias plataformas digitais regulam, em seus termos de uso, sem uma uniformidade, a destinação dos conteúdos digitais de usuários falecidos, conferindo, no momento da adesão em vida, pelos ditos usuários, às referidas plataformas, opções pré-determinadas a serem escolhidas. Caso, ao aderirem aos termos de uso, os usuários não se atentem à escolha de uma das opções disponíveis na plataforma, em regra, com o seu falecimento, o conteúdo não será transmissível.

Como se não bastasse a limitação da liberdade de escolha dos usuários quanto à disposição, em vida, acerca da destinação de seus bens digitais, já que nem sempre as opções oferecidas pela plataforma convergem com a vontade do usuário, não raras as vezes os usuários aderem aos termos de uso sem sequer se inteirarem de suas disposições.

Logo, ao invés de propiciarem, mediante seus termos e políticas de uso, a manifestação de vontade do titular sobre a manutenção ou não da privacidade dos conteúdos por ele inseridos, as plataformas obstam o respeito à autonomia da vontade de referido titular. Tal comportamento representa autêntica violação às normas protetivas aos direitos do consumidor, não se sustentam, pois, diante do ordenamento jurídico brasileiro[52].

---

monta a certas e determinadas pessoas, ou, indeterminadamente, aos pobres de certo lugar, assim como legar móveis, roupas ou jóias, de pouco valor, de seu uso pessoal".

51. Sobre o *SecureSafe*, consultar: https://www.securesafe.com/en/data-inheritance. Acesso em: 28 fev. 2023.

52. Nesse sentido, Fernanda Mathias de Souza Garcia esclarece que: "*[...] os termos de uso das*

Partindo dessas premissas, é inegável que, no confronto entre disposições testamentárias de um determinado titular de bens digitais e os termos de uso de dada plataforma digital por ele utilizada, as primeiras, ao propiciarem o pleno exercício da autonomia privada, prevalecem sobre estes últimos.

Superada essa questão, resta o desafio da avaliação do acerto digital, de suma importância não só para fins de tributação da herança, mas também, para a verificação do respeito à legítima dos herdeiros.

Isso porque, de acordo com o art. 1.789 do Código Civil, havendo herdeiros necessários (descendentes, ascendentes, cônjuge e companheiro), o testador somente poderá dispor de metade da herança, de modo que se deve resguardar a legítima daqueles[53]. Nesse contexto, a avaliação do acervo digital com valor econômico, em especial daquele que tenha um duplo aspecto (patrimonial e existencial), é fundamental para que não haja a violação à legítima dos herdeiros.

No caso dos bens digitais com valor econômico, é possível avaliá-los tendo por referência o preço de negociação no mercado de bens similares, na data de falecimento do titular. A título exemplificativo, no tocante às criptomoedas, pode-se adotar como critério o valor de cotação na data do óbito.

Contudo, a maior dificuldade dá-se quanto ao acervo digital de cunho patrimonial e existencial, como, por exemplo, os canais no *Youtube* e as contas exploradas no *Instagram* e *Facebook*. Com efeito, "*o nicho de mercado é pequeno e a avaliação de cada página ou canal é extremamente variável, dependendo, literalmente, do caso*

---

plataformas de internet *também se submetem à boa-fé objetiva e às normas de ordem pública do ordenamento pátrio. Com isso, 'permite-se a declaração de nulidade das cláusulas do contrato de adesão que impeçam a transmissão da conta aos herdeiros e que esvaziem princípios basilares do direito sucessório, frustrando o fim último do contrato' (MENDES; FRITZ, 2019, p. 206). Entender de modo diverso é assumir que os dados digitais ficariam à mercê e sob a propriedade das próprias plataformas, o que parece inconcebível. Uma vida inteira contratual não pode ser entregue ao poder das empresas digitais, pois o fato de o serviço prestado pelo provedor de* internet *ser gratuito não desvirtua a relação de consumo, constante do art. 3º, §2º, do CDC, cuja interpretação deve ser a mais ampla possível*". (GARCIA, Fernanda Mathias de Souza. *Herança digital:* o direito brasileiro e a experiência estrangeira. 2. ed. Rio de Janeiro: Lumen Juris, 2022. p. 123. *E-book*).

53. O art. 1.845 do Código Civil dispõe: "*São herdeiros necessários os descendentes, os ascendentes e o cônjuge*". Apesar de referido dispositivo não fazer menção ao companheiro e à companheira, eles se equiparam ao cônjuge para tal finalidade.

concreto"[54].

Considerando essa dificuldade, Daniel Bucar e Caio Ribeiro Filho sugerem uma metodologia interessante, aproximando a avaliação dessas situações patrimoniais/existenciais daquela efetivada para se apurar o valor de ativos intangíveis de sociedades empresárias contratuais, como a sociedade limitada[55].

Não há dúvidas de que a metodologia sugerida pode contribuir para a solução do problema relativo à avaliação dos bens aqui tratados, servindo de parâmetro para nortear o planejamento sucessório da herança digital.

54. BUCAR, Daniel; PIRES, Caio Ribeiro. Situações patrimoniais digitais e ITCMD: desafios e propostas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 442. *E-book*.

55. Segundo aludidos autores: "*A aproximação da avaliação de contas monetizadas com aquela empreendida com o fim de estabelecer o valor do ativo intangível de uma sociedade parece bem se adequar à hipótese, também pelo fato de o conteúdo divulgado por* influencers*,* youtubers *e outros mais, guardar certa equiparação a uma propriedade intelectual, sendo, portanto, comparável a uma obra protegida por direitos autorais (Art. 7º da Lei n. 9.610/98). Assim, as receitas adquiridas com base nesse trabalho, estão próximas – ou, até, se igualam – às remunerações devidas por uso da obra ou marca criada*". (BUCAR, Daniel; PIRES, Caio Ribeiro. Situações patrimoniais digitais e ITCMD: desafios e propostas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 446. *E-book*). Ainda sobre essa questão, ditos autores destacam as instruções constantes do Comitê de Pronunciamentos Contábeis 04, relativo a ativos intangíveis. Como elucidam, "*conceitos expostos no documento podem ser fundamentais na avaliação dos perfis explorados economicamente. O principal deles é o de 'vida útil determinada', imprescindível para compreender o verdadeiro aproveitamento cujo herdeiro conseguirá extrair da riqueza digital acumulada, ao receber um perfil do qual o falecido se valia para fins econômicos. Em outras palavras, ao analisar-se uma página que recebe, constantemente, conteúdo de seu titular quando esse morre é necessário pensar (a) o quanto seu conteúdo ainda será reproduzido, (b) quanto tempo irá levar para os acessos diminuírem. A partir de tais diretivas, de caráter geral, traçam-se dois parâmetros específicos, capazes de auxiliar a fixação do valor de mercado de uma conta monetizada, os quais também se baseiam na concepção de que esses bens são centros de imputação de diversas relações jurídicas patrimoniais*". (BUCAR, Daniel; PIRES, Caio Ribeiro. Situações patrimoniais digitais e ITCMD: desafios e propostas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 446. *E-book*).

6. CONCLUSÃO

Partindo-se do estudo realizado, vê-se que a herança digital traz inúmeros desafios, os quais se tornam ainda mais complexos diante da ausência de regulação específica acerca da matéria.

Diante desse cenário, não existem respostas prontas para as novas questões jurídicas suscitadas no campo sucessório brasileiro, as quais vêm sendo enfrentadas casuisticamente, a partir dos vetores principiológicos da Constituição de 1988, em especial, a dignidade da pessoa humana. Sob esse prisma, liberdade e privacidade do titular dos bens digitais são facetas de realização da dignidade da pessoa humana que devem ser sopesadas em concreto, evitando-se eventuais distorções que possam comprometer a própria proteção à personalidade.

Não obstante a pluralidade de projetos legislativos abarcando a herança digital e a despeito da certeza de que as inovações tecnológicas demandam um repensar do sistema jurídico como um todo, é indispensável o aprofundamento das reflexões sobre o tema, antes de engessá-lo em normas jurídicas que podem não representar a tutela mais adequada dos direitos da personalidade.

REFERÊNCIAS

ABREU, Renata. *Projeto de Lei n. 1.144, de 2021*. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1982888&filename=Tramitacao-PL%201144/2021. Acesso em: 27 fev. 2023.

ADOLFO, Luiz Gonzaga Silva; KLEIN, Júlia Schroeder Bald. Herança digital: diretrizes a partir do *leading case* do *Der Bundesgerichtshof*. *In: Revista brasileira de direito civil*. Belo Horizonte, v. 30, p. 183-199, out./dez. 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/687/502. Acesso em: 25 fev. 2023.

BEVILÁQUA, Clóvis. *Direito das sucessões.* 5. ed. rev. e atual. Rio de Janeiro: Francisco Alves, 1955.

BRASIL. *Constituição da República Federativa do Brasil de 1988, de 5 de outubro de 1988.* Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 fev. 2023.

BRASIL. *Lei n. 10.406, de 10 de jan. de 2002*. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 25 fev. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 4.099, de 2012*. Altera o art. 1.788 da Lei n. 10.406, de 10 de janeiro de 2002, que 'institui o Código Civil'. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1004679&filename=Tramitacao-PL%204099/2012. Acesso em: 27 fev. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 4.847, de 2012*. Acrescenta o Capítulo II-A e os arts. 1.797-A a 1.797-C à Lei n. 10.406, de 10 de janeiro de 2002. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1049733&filename=Tramitacao-PL%204847/2012. Acesso em: 27 fev. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 5.820, de 2019.* Dá nova redação ao art. 1.881 da Lei no 10.406, de 2002, que institui o Código Civil. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1829027&filename=Tramitacao-PL%205820/2019. Acesso em: 27 fev. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 3.050, de 2020.* Altera o art. 1.788 da Lei n. 10.406, de 10 de janeiro de 2002. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1899763. Acesso em: 27 fev. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 3.051, de 2020.* Acrescenta o art. 10-A à Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), a fim de dispor sobre a destinação das contas de aplicações de internet após a morte de seu titular. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1899766&filename=Tramitacao-PL%203051/2020. Acesso em: 27 fev. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 2.664, de 2021.* Acrescenta o art. 1857-A à Lei n. 10.406, de 2002, Código Civil, de modo a dispor sobre a herança digital. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2049837&filename=PL%202664/2021. Acesso em: 27 fev. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 703, de 2022.* Acrescenta o art. 1857-A à Lei n. 10.406, de 2002, Código Civil. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2152405&filename=PL%20703/2022. Acesso em: 27 fev. 2023.

BRASIL. Senado Federal. *Projeto de Lei n. 6.468, de 2019.* Altera o art. 1.788 da Lei n. 10.406, de 10 de janeiro de 2002, que institui o Código Civil, para dispor sobre a sucessão dos bens e contas digitais do autor da herança. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8056437&ts=1674176579296&disposition=inline. Acesso em: 27 fev. 2023.

BRASIL. Tribunal de Justiça do Estado de Minas Gerais. Processo n. 0023375-92.2017.8.13.0520. Vara Única da Comarca de Pompeu. Juiz Manoel Jorge de Matos Júnior. Julgado em 08 jun. 2018. Disponível em: https://www.tjmg.jus.br. Acesso em: 26 fev. 2023.

BRASIL. Tribunal de Justiça do Estado de Minas Gerais. 3ª Câmara Cível. Agravo de Instrumento n. 1.0000.21.190675-5/001. Relatora Des. Albergaria Costa. Julgado em 27 jan. 2022. Disponível em: www.tjmg.jus.br. Acesso em: 27 fev. 2023.

BRASIL. Tribunal de Justiça do Estado de São Paulo. 31ª Câmara Cível de Direito Privado. Apelação

Cível n. 1119688-66.2019.8.26.0100. Relator Des. Francisco Casconi. Julgado em 09 mar. 2021. Disponível em: www.tjsp.jus.br. Acesso em: 27 fev. 2023.

BRASIL. Tribunal de Justiça do Estado de São Paulo. 7ª Câmara Cível de Direito Privado. Apelação Cível n. 100433442.2017.8.23.0268. Relator Des. Rômulo Russo. Julgado em 31 mar. 2021. Disponível em: www.tjsp.jus.br. Acesso em: 27 fev. 2023.

BRASIL. Tribunal de Justiça do Mato Grosso do Sul. Processo n. 0001007-27.2013.8.12.0110. 1ª Vara do Juizado Especial Central de Campo Grande. Juíza Vânia de Paula Arantes. Julgado em 19 mar. 2013. Disponível em: https://www.migalhas.com.br/arquivo_artigo/art20130424-11.pdf. Acesso em: 26 fev. 2023.

BUCAR, Daniel; PIRES, Caio Ribeiro. Situações patrimoniais digitais e ITCMD: desafios e propostas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 433-457. *E-book*.

COSTA FILHO, Marco Aurélio de Farias. *Patrimônio digital:* reconhecimento e herança. Recife: Nossa Livraria, 2016.

FROTA, Pablo Malheiros da Cunha. *Parecer jurídico,* de 12 de dez. 2017. Disponível em: https://www.iabnacional.org.br/pareceres/pareceres-votados/016-2017. Acesso em: 27 fev. 2023.

GARCIA, Fernanda Mathias de Souza. *Herança digital:* o direito brasileiro e a experiência estrangeira. 2. ed. Rio de Janeiro: Lumen Juris, 2022. *E-book*.

GONÇALVES, Laura Marques. *Transmissão* post mortem *de patrimônio digital:* em defesa da ampla sucessão. Dissertação apresentada ao Programa de Pós-Graduação da Faculdade de Direito da Universidade Federal de Minas Gerais, 2021. Disponível em: https://repositorio.ufmg.br/handle/1843/41742. Acesso em: 22 fev. 2023.

HONORATO, Gabriel; LEAL, Lívia Teixeira. Exploração econômica de perfis de pessoas falecidas: reflexões jurídicas a partir do caso Gugu Liberato. *In: Revista brasileira de direito civil*. Belo Horizonte, v. 23, p. 163-164, jan./mar. 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/523/350. Acesso em: 25 fev. 2023.

KONDER, Nelson; TEIXEIRA, Ana Carolina Brochardo. O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina Brochardo. São Paulo: Foco, p. 40-72. *E-book*.

LEAL, Livia Teixeira. *Internet e morte do usuário:* propostas para o tratamento jurídico *post mortem* do conteúdo inserido na rede. Rio de Janeiro: LMJ Mundo Jurídico, 2018.

LÔBO, Paulo. *Direito civil:* parte geral. 5. Ed. São Paulo: Saraiva, 2015.

NEVARES, Ana Luiza. *A sucessão do cônjuge e do companheiro na perspectiva do direito civil constitucional.* 2. ed. São Paulo: Atlas, 2015.

OLIVEIRA, Camila Helena Melchior Baptista de; TEPEDINO, Gustavo. *Streaming* e herança digital. *In: Herança digital*: controvérsias e alternativas. LEAL, Lívia Teixeira; TEIXEIRA, Ana Carolina

Brochardo. São Paulo: Foco, p. 122-154. *E-book*.

SECURESAFE. https://www.securesafe.com/en/data-inheritance. Acesso em: 28 fev. 2023.

SOARES, Flaviana Rampazzo; BASTOS, Ísis Boll de Araujo. *Avanços tecnológicos e proteção* post mortem *dos direitos de personalidade por meio do testamento*. Revista Fórum de Direito Civil – RFDC | Belo Horizonte, ano 4, n. 10, p. 189-205, set./dez. 2015.

TAVEIRA JR., Fernando. *Bens digitais (digital assets) e a sua proteção pelos direitos da personalidade:* um estudo sob a perspectiva da dogmática civil brasileira. Porto Alegre: Revolução eBooks – Simplíssimo, 2018.

IOT E METAVERSO:
CONEXÃO COMO LEMA

Pietra Daneluzzi Quinelato

Doutoranda em Direito Civil na Universidade de São Paulo. Coordenadora de Direito Digital do Mansur Murad Advogados.

Aluísio de Freitas Miele

Mestre em Direito e Desenvolvimento pela Universidade de São Paulo. Sócio no Miele e Manini Sociedade de Advogados.

DOI: https://doi.org/10.59224/dti5.ch16

Resumo: O cenário tecnológico vivenciado não é apenas disruptivo. Esta quebra do "percurso normal" é diária e traz, nesta mesma velocidade, inovações que proporcionam novas oportunidades e criam melhorias para a vida em sociedade, em paralelo à criação de fissuras como no que diz respeito à proteção de dados pessoais. Neste sentido, por meio de abordagem metodológica qualitativa e documental indireta, o presente artigo aborda o conceito da IoT e suas aplicações, o universo imersivo do metaverso, a interação entre esses dois ecossistemas e a necessidade de (re)pensar a arquitetura jurídica digital. Para tanto, demonstrou-se como a web3, ao prometer um ambiente descentralizado, seguro e global, contribui para uma realidade cada vez mais imersiva e permite a interação entre IoT e metaverso. Neste universo imersivo, em que "coisas" se conectam entre si e com o indivíduo, intensifica-se a quantidade de dados pessoais coletados, principalmente pelos *wearables*. Assim, medidas de transparência e ética, além de garantias aos direitos fundamentais devem acompanhar todo este desenvolvimento tecnológico.

Palavras-chave: Internet das Coisas; Metaverso; Proteção de Dados Pessoais.

Abstract: *The technological scenario experienced is not only disruptive. This break from the "normal path" is daily and brings, at the same speed, innovations that provide new opportunities and create improvements for life in society, in parallel with the creation of fissures as regards data protection. In this sense, through an indirect qualitative and documental methodological approach, this article addresses the concept of IoT and its applications, the immersive universe of the metaverse, the interaction between these two ecosystems and the need to (re)think the digital legal architecture. We demonstrated how web3 contributes to an increasingly immersive reality and allows interaction between IoT and metaverse. In this online and immersive universe, in which "things" connect with each other and with individuals, the amount of personal data collected is intensified, mainly by wearables. Thus, transparency and ethics measures, in addition to guarantees of fundamental rights, must accompany all this technological development.*

Keywords: *Internet of Things; Metaverse; Data Protection; Digital Law.*

Sumário: 1. Introdução; 2. IoT: do conceito às possibilidades de aplicação; 3. Metaverso: imersão como objetivo final; 4. Iot e Metaverso: interação, aplicação e proteção de dados pessoais; 5. Considerações finais; Referências.

1. INTRODUÇÃO

Quando Nikola Tesla[1] previu que seríamos capazes de nos comunicar de forma instantânea, independentemente da distância, ao citar inclusive que ouviríamos e veríamos uns aos outros como se estivéssemos presencialmente por meio de um instrumento que caberia no bolso de um colete, talvez não tivesse vislumbrado o avanço da tecnologia para debates envolvendo implicações e interações da blockchain, Web3, IoT (Internet das Coisas), NFTs (tokens não-fungíveis)[2] e metaverso no ecossistema digital[3]. Tampouco é possível afirmar que Kevin Ashton, quando utilizou o termo Internet of Things (Internet das coisas – IoT) pela primeira vez, tinha total confiança e clareza qual, de fato, seria a importância da hiperconectividade para a evolução tecnológica.

1. KENNEDY, John B. *When Woman is boss*. 30/01/1926. Disponível em: https://teslauniverse.com/nikola-tesla/articles/when-woman-boss. Acesso em: 27 mar. 2023. "Quando o wireless for perfeitamente aplicado, toda a terra será convertida em um enorme cérebro, o que de fato é, todas as coisas sendo partículas de um todo real e rítmico. Seremos capazes de nos comunicar uns com os outros instantaneamente, independentemente da distância. Não apenas isso, mas através da televisão e da telefonia veremos e ouviremos uns aos outros tão perfeitamente como se estivéssemos face a face, apesar das distâncias intermediárias de milhares de milhas; e os instrumentos através dos quais seremos capazes de fazer sua vontade são incrivelmente simples comparados com nosso telefone atual, um homem poderá carregar um no bolso do colete." (tradução dos autores)
2. É um arquivo digital registrado em blockchain, ou seja, uma chave eletrônica geradora de códigos, permitindo uma assinatura digital totalmente imutável. O NFT pode ser uma obra de arte, um avatar, uma bolsa, uma figurinha rara que são registrados em digital wallets e podem ser vendidos por meio de transferência para uma outra wallet (assim como ocorre com a criptomoeda).
3. O termo ecossistema digital é utilizado neste artigo para tratar da revolução tecnológica 4.0, das suas ferramentas (Web´s, IoT, metaverso, interoperabilidade, conectividade e da interação que dentro, e entre todos eles, ocorrem, incluindo, por óbvio, o Direito Digital e as políticas públicas.

Diante da imparável marcha tecnológica, a IoT se apresenta como uma ferramenta central deste ecossistema digital, uma vez que promove a conectividade de milhares de dispositivos e estabelece uma nova arquitetura de computação ubíqua[4]. Floresce-se, assim, a capacidade dos objetos se comunicarem de forma independente, onipresente, como verdadeiros provedores de serviços capazes de fortalecer a ideia de estar em rede e de alimentarem uma pluriconectividade nas cidades, veículos, residências e indústrias.

A possibilidade de linkar o mundo físico à internet, a outras redes de dados ou mesmo a outras IoT´s performa uma verdadeira mudança na sociedade e na economia[5], principalmente no que diz respeito ao metaverso. Novas disposições de dados, protocolos de segurança, *digital twins* e realidade aumentada definem a importância da interação entre IoT e metaverso. A evolução dos ambientes virtuais com a finalidade de reproduzir de forma mais próxima a realidade é potencializada por meio de processamento de dados de IoT consumidos em tempo real pelo metaverso. Em outras palavras, a IoT permite que o metaverso encontre sua plenitude, construindo um ambiente totalmente imersivo ao usuário, e esta própria evolução do metaverso impacta na evolução e desenvolvimento da IoT, demandando arquiteturas mais aprimoradas.

Neste cenário de pluralidade de tecnologias, as experiências (trabalhar, estudar, comprar um imóvel, comprar uma roupa, constituir uma empresa, contemplar uma obra de arte, participar de eventos e shows) são cada vez mais digitais, descentralizadas e imersivas. Surgem novos comportamentos, e os desejos e os hábitos das pessoas alteram-se. Em paralelo, o comportamento de gerações também molda (e moldará)

4. Também compreendida como computação pervasiva, o termo representa a definição da integração das diversas tecnologias/dispositivos de forma "onipresente" no nosso cotidiano. Basta pensar na relação que podemos ter com um grande número de dispositivos inteligentes e o modo como estes interagem entre si e conosco em qualquer local e momento.
5. A Consulta Pública do Ministério da Ciência, Tecnologia, Inovações e Comunicações (Câmara IoT) trouxe que são mais de 15 bilhões de dispositivos conectados no mundo, podendo atingir cerca de 35 bilhões de dispositivos no ano de 2025. (BRASIL. da Ciência, Tecnologia, Inovações e Comunicações. *Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil*: Consulta Pública. Dez. 2016. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.abinee.org.br/informac/arquivos/aiot.pdf. Acesso em: 26 mar. 2023.

novas invenções tecnológicas. Portanto, se de um lado as novas tecnologias demandam novos comportamentos, novos comportamentos demandam novas tecnologias. Todas estas adaptações que causam disrupções e quebra de paradigmas alteram as mais diversas soluções jurídicas aplicáveis[6] e fazem (re)pensar a arquitetura jurídica digital.

Neste artigo, trouxemos considerações iniciais sobre IoT, visando demonstrar seus impactos na interatividade da sociedade atual, bem como os novos horizontes possibilitados pela tecnologia, sem intuito de esgotar o tema. Também foram abordados conceitos relacionados à Web3, antes de definir metaverso e explicar a importância da imersão do usuário nesse novo ambiente "phygital" (físico e digital). Por fim, mostrou-se que a IoT permitirá que as experiências do metaverso alcancem seu maior potencial em conectividade e imersão, sem se descurar de algumas questões que nos são apostas como questões atinentes à proteção de dados pessoais dos usuários nesse ambiente.

2. IOT: DO CONCEITO ÀS POSSIBILIDADES DE APLICAÇÃO

No início da utilização dos computadores, bem como com a internet "discada", a interação com os usuários era totalmente estática. Em princípio, a internet surgiu para criar um sistema de comunicação inviolável diante dos ataques nucleares para, após, permitir o empacotamento de mensagens pelos próprios indivíduos sem a necessidade de um centro de controle, além de alcançar um sistema de comunicação global horizontal altamente tecnológico.

Esta capacidade só foi possível a partir do momento em que os computadores puderam "dialogar" uns com os outros por meio do protocolo de transmissão TCP/IP. Como explica o sociólogo Castells, "sua flexibilidade permitia a adoção de uma estrutura de camadas múltiplas de links entre redes de computadores, o que demonstrou sua capacidade de adaptar-se a vários sistemas de comunicação e a uma diversidade de códigos"[7]. Com o movimento contracultural nos Estados Unidos da

6. CENDÃO, Fábio; ANDRADE, Lia. *Direito, metaverso e NFTs*: introdução aos desafios na web3. São Paulo: ExpressaJur, 2022.

7. CASTELLS, Manuel. *A sociedade em rede*. 8.ed. v. 1. Trad. Roneide Venancio Majer. São Paulo: Paz e Terra, 1999. p. 82-84. Este protocolo TCP/IP representa a sua divisão em protocolo inter-

América na década de 1960, que desenvolveu tecnologia "fora" do Pentágono, surgiu o modem para computador, que permitiu a transferência direta de arquivos entre computadores[8]. Diante da grande revolução tecnológica do final do século XX, os computadores passaram a caber literalmente no bolso, ou seja, o uso da internet móvel superou o uso dos desktops.

Nos dias de hoje, este diálogo avançou e não se dá apenas no âmbito de dois computadores, mas sim em um ecossistema em que "coisas" se comunicam e se conectam e com outros dispositivos habilitados para web, como veremos no cenário da Web3.

A cada dia, mais veículos, mais cidades, eletrodomésticos, residências, máquinas e equipamentos estão conectados à internet para praticar ações a partir de informações e dados recebidos. São inúmeros dispositivos interconectados e conectados à internet sem a interação homem-máquina ou homem-homem. É exatamente esta conectividade entre bens que conforma e conceitua a Internet das Coisas.

> Do ponto de vista da normalização técnica, a IoT pode ser vista como uma infraestrutura global voltada para a era digital, permitindo serviços avançados por meio da interconexão de coisas (físicas e virtuais) com base nas tecnologias de informação e comunicação interoperáveis existentes e em constante evolução.[9]

O que se pode dizer, em outras palavras, é que *coisas* passam a adquirir

---

redes (IP) e servido-a-servidor (TCP). A sua importância é visível ainda nos dias atuais quando textos recentes definem IoT com base neste protocolo: "The semantic origin of the expression is composed by two words and concepts: "Internet" and "Thing", where "Internet" can be defined as "The world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP)", while "Thing" is "an object not precisely identifiable" Therefore, semantically, "Internet of Things" means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols". (BASSI, A.; HORN, G. Internet of Things in 2020: A Roadmap for the Future. European Commission: Information Society and Media, v. 22, p. 97-114, 2008. p. 4. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://docbox.etsi.org/erm/Open/CERP%2020080609-10/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v1-1.pdf. Acesso em: 27 mar. 2023).

8. Op. cit. p. 87.
9. MAGRANI, Eduardo. *A internet das Coisas*. São Paulo: Editora FGV, 2018. p. 45. Disponível em: chrome-

"personalidade" (ainda que virtual, mas não com os efeitos jurídicos) ou identidades, em um claro sentido de somar funcionalidades inteligentes capazes de se conectar e se comunicar nos mais distintos contextos. Dessa forma, *coisas* passam a ser muitas outras coisas como *smart cities, smart clothes, Industrial IoT e Consumer IoT*. Dentre estes objetos interconectados é possível elencar: software, cloud, roteadores, smartphones, *wearables* (dispositivos vestíveis). Em verdade, muitos objetos (dispositivos ou mesmo "coisas") se transmudaram para dispositivo de comunicação sem fio com tráfego de dados a partir do momento que passaram a fazer transmissão.[10]

Pode-se dividir a aplicação de IoT em duas demandas verticalizadas, a pública e a privada. Na pública as possíveis aplicações incluem gestão de infraestrutura pública e cidades inteligentes, melhoria no serviço de saúde (gestão de distribuição de medicamento; monitoramento de pacientes; informatização do SUS), meio ambiente (monitoramento de qualidade do ar, água; prevenção e detecção de desastres naturais, rastreabilidade de produtos), e também educação (plataformas de ensino; elaboração de conteúdo pedagógicos).[11]

No âmbito privado a IoT pode ser aplicada nos setores da saúde (monitoramento preventivo de sinais vitais e alertas automatizados para o hospital ou médicos; teleatendimento, controle de cadeia frio de vacinas e remédios; quartos inteligentes que integram com o paciente por meio de IoT e computação cognitiva; realidade virtual para treinamento médico); da agricultura (racionalizar, reduzir e otimizar perdas do plantio; irrigação inteligente; redução de perdas devido ao clima; controle automatizado da qualidade de alimentos); da infraestrutura (construção de prédios, indústrias, residências e comércios inteligentes); no setor automotivo (veículos autônomos e inteligentes; comunicação veículo à veículo); de bens de consumo e varejo (identificação e monitoramento do comportamento do consumidor; tecnologia vestíveis – *wearables* para bem-estar e monitoramento da saúde; omni-channel viabilizado pela

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 26 mar. 2023.

10. BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Consulta pública*: Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil, dez. 2016, p. 13.
11. Op. cit., p. 66.

digitalização); de telecomunicação e mídia (jogos em realidade virtual; shows e esportes interativos ao vivo); da indústria (máquinas e equipamentos conectados para a redução de perdas e paradas em produção; uso de especialistas remotos para reparos em campo); em escritórios e residências inteligentes (luzes, geladeiras, televisões e máquinas interconectadas por meio de um comando central, como a Alexa (Amazon)).[12]

Uma das indústrias que acompanha de forma célere todo esse ecossistema de inovação é a da moda[13], a partir da tendência da tecnologia vestível, como relógios (*smartwatches*), sapatos, óculos, camisetas e outras peças de vestuário. Estas tecnologias produzem informações sobre os usuários e podem alterar a cor do bem, monitorar atividade física ou mesmo proporcionar imersão na própria realidade.

No que diz respeito ao contexto normativo brasileiro, há muito o que discutir e evoluir[14]. A princípio, menciona-se as taxas de fiscalização, de instalação e funcionamento das estações de telecomunicações que integram sistemas de comunicação máquina a máquina[15], a Criação da Câmara IoT que iniciou estudos sobre políticas de desenvolvimento e fomento da IoT que culminou na Consulta Pública no ano de 2016 e o Decreto n.º 9.854/2019[16].

Nesse contexto, é possível elencar algumas vulnerabilidades da IoT com necessidade de endereçamento, como eventual falta de encriptação para transporte na rede

12. Op. cit., p. 70-75.
13. O Direito da Moda (*Fashion Law*) e sua regulação possui um campo de estudo e de prática específico, mesmo que não tão (re)conhecido. Sobre o tema, cf. DOMINGUES, Juliana Oliveira; MIELE, Aluísio de Freitas; QUINELATO, Pietra Daneluzzi; HERNANDES, Beatriz; RAFIH, Rhasmye El. **Fashion Law**: o direito está na moda. São Paulo: Singular, 2019.
14. Recomenda-se a leitura de FALEIROS JR., José Luiz de Moura. Responsabilidade por falhas de algoritmos de inteligência artificial: ainda distantes da singularidade tecnológica, precisamos de marcos regulatórios para o tema? *Revista de Direito da Responsabilidade*, ano 4, 2022. Disponível em: https://www.academia.edu/88822610/Responsabilidade_por_falhas_de_algoritmos_de_intelig%C3%AAncia_artificial_ainda_distantes_da_singularidade_tecnol%C3%B3gica_precisamos_de_marcos_regulat%C3%B3rios_para_o_tema. Acesso em 20 mar. 2023.
15. Lei n.º 12.715 de 2012, artigo 38 com alteração proporcionada pela Lei n.º 14.108/2020.
16. Não é escopo do presente artigo avançar no debate acerca deste decreto, mas é preciso enfatizar que há um certo grau de generalidade e precisa de novas regulações para o alcance dos objetivos apresentados.

local, nuvem ou internet; proteção inadequada de software; consentimento insuficiente; interface web insegura e questões relacionadas à privacidade dos indivíduos e proteção de dados pessoais dos usuários/consumidores.17 Tão logo, a sua regulação deve equilibrar e condensar os interesses do mercado e da própria sociedade a partir desses avanços tecnológicos com a tutela do consumidor; o que pode ser alcançado a partir de controle, transparência, consentimento e oposição ao processo automatizado. Nesta linha, a regulação deve "incentivar o uso de metodologias diferenciais de privacidade, como pseudonimização, anonimização ou criptografia, o que reduziria os riscos de segurança cibernética e as obrigações com notificação de violação de dados"[18].

O crescimento e a evolução das plataformas IoT, aliados ao grande fluxo de dados que podem fornecer, servirão também para a aplicação de um metaverso cada vez mais descentralizado e capaz de fornecer uma sociedade mais interconectada e imersiva. A interoperabilidade entre IoT e realidade aumentada poderá desbloquear novos aplicativos que, por sua vez, auxiliarão na solução dos problemas do mundo real, tanto a nível pessoal quanto a nível social. É o que será apresentado no terceiro capítulo.

3. METAVERSO: A IMERSÃO COMO OBJETIVO FINAL

Antes de falarmos sobre o metaverso, mostra-se importante a breve conceituação da Web3, pautada na tecnologia blockchain. Como mencionado acima, a primeira conexão ocorreu no final da década de 1960, tendo a ARPANET como a precursora da internet que utilizamos hoje. Criada, portanto, em um contexto de Guerra Fria, nascia a web 1.0, que se popularizou na década de 90 ao oferecer uma conexão "discada" para um conteúdo linear e estático, sem possibilidade de interação do usuário.

Nos anos 2000, com o avanço das redes sociais, caracteriza-se a web 2.0 diante da possibilidade de interação entre usuários e demais *players*, pela possibilidade de criação de conteúdo pelo próprio usuário "prosumidor" (que produz e consome) e a

17. BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Consulta pública*: Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil, dez. 2016, p. 13.

18. MAGRANI, Eduardo. *A internet das Coisas*. São Paulo: Editora FGV, 2018. p. 91.

utilização de palavras-chave indexadoras. Nesse cenário, usuários ganham voz, comentando sobre marcas, produtos e serviços adquiridos, recomendando ou criticando empresas. Estas, por sua vez, exploram um marketing direcionado, possibilitado pela análise de perfis de consumo dos usuários, a partir do seu comportamento *online*. Com essa tecnologia, aumenta-se a coleta e o processamento de dados pessoais, direciona-se conteúdo, explora-se a publicidade comportamental e a personalização de produtos e serviços.

A Web3, com raízes nos anos 2010 e no surgimento das criptomoedas, está ainda em sua infância, mas com um futuro promissor. Ao prometer um ambiente seguro, descentralizado (ou seja, sem uma entidade hierárquica central) e global, permitirá que usuários explorem diversas funcionalidades, incluindo lazer, investimento, trabalho e comunicação.

Nessa nova geração da web, usuários conectam-se por meio de uma carteira digital, conhecida como wallet (ex. MetaMask)[19], que os insere no universo dos tokens não fungíveis, dos diferentes mundos de metaverso, das criptomoedas e finanças descentralizadas, também chamadas de DeFi.

Vale mencionar que, apesar de referida *wallet* ter um código complexo e extenso a ela atribuído, que depende da escolha do usuário para ser identificada como pertencente a um indivíduo, trata-se de um dado pseudonimizado. Essa categorização é importante para afastar eventuais questões sobre a inaplicabilidade das legislações de proteção de dados pessoais às informações desse ecossistema. Nesse sentido, Ruiz explica o conceito de pseudonimização como:

> [...] uma técnica que substitui informações contidas num conjunto de dados que identifica um indivíduo por um identificador artificial, um pseudônimo. Consideremos um conjunto de dados formados por dois tipos de dados, os dados pessoais, tais como nome e endereço, e demais dados que não singularizam a pessoa. Na pseudonimização, os dados pessoais são substituídos por um identificador artificial e mantidos num banco de dados separado que liga dados pessoais e pseudônimo. Enquanto isso, os

19. Muitos mundos de metaverso, por exemplo, têm interface com a web 2.0 ou ainda não estão no ambiente descentralizado da Web3, sendo necessário um login com e-mail e senha para usufruir dos seus benefícios. Como exemplo, tem-se a plataforma Roblox, ainda organizada de modo centralizado, mas que já remete a essa nova fase da web que está sendo construída.

> demais dados relativos à pessoa são referenciados por este pseudônimo e mantidos numa segunda base de dados. Desta maneira o processo de reidentificação só ocorre com a junção das duas bases de dados, ou seja, da base com os pseudônimos que os associa aos dados pessoais e os demais registros.

Mas as *wallets* não são a única ferramenta de interação com o universo da Web3, cenário no qual se destacam os *wearables* e a IoT, como óculos de realidade aumentada, tecidos que simulam sensações no corpo, dispositivos com tecnologia olfativa, entre outros. Portanto, ainda que se possa considerar que o conceito de Web3 é fluído, a principal distinção com as outras gerações da web é que possibilita de modo mais imersivo a conexão entre objetos e objetos com pessoas, aproximando-se da IoT.

Nesse contexto, mundos de metaverso permitem que usuários tenham experiências imersivas, interagindo em tempo real por meio de seus avatares. Espera-se que, nos próximos dez anos, essas tecnologias (Web3 e IoT) permitam uma convergência de mundos virtuais e reais, em que indivíduos poderão acessar conteúdo digital ao andarem nas ruas, por exemplo, ou de seus sofás em casa, por meio de *wearables*.

A integração entre IoT e metaverso permitirá, portanto, novas e inúmeras oportunidades para a indústria, prestação de serviços, bem como para necessidades pessoais e também aquelas de cariz social. Isto porque, será possível que os espaços virtuais passem a interagir e acessar o mundo real de forma instantânea com uma vasta gama de dados, enquanto o metaverso pode oferecer a interface de usuário 3D para o *cluter* de dispositivo IoT.[20]

Alguns livros simulam esse cenário futurista, como Kiss me First de Lottie Moggach e Ready Player One de Ernest Cline, que foram produzidos cinematograficamente e disponibilizados na plataforma de streaming Netflix. Outras séries também tratam da temática por meio da demonstração da utilização de *wearables* e imersão do usuário, como Upload e Periféricos, disponíveis na Amazon Prime Video.

Mas vale mencionar que apesar de o tema ser tratado como "o" metaverso, a

20. BLOCKCHAIN CONCIL. *How Will IoT Integrate The Real World With The Metaverse?* Set., 2022. Disponível em: https://www.blockchain-council.org/metaverse/how-will-iot-integrate-the-real-world-with-the-metaverse/#:~:text=The%20combination%20of%20Metaverse%20and,virtual%20experiences%20to%20its%20users. Acesso em: 25 mar. 2023.

tecnologia não se trata de uma unidade atualmente, pois não há interligação entre os mundos de metaverso. Existem diversas plataformas disponíveis para os usuários, como Decentraland, Fortnite, Second Life, Microsoft Mesh, Horizon Worlds, entre outras. Elas permitem que os usuários participem de diversas experiências, como shows, reuniões, aulas, encontros, jantares, compras, passeios e conversas, nas quais serão tratados dados pessoais. No entanto, o usuário ainda não pode circular entre elas livremente. Seus ativos adquiridos em uma não se conectam com as demais.

Contudo, esse cenário tende a evoluir para um ambiente ainda mais descentralizado, com maior exploração de *wearables* a partir da sua popularização. Conforme estudo da Gartner, em 2026, cerca de um quarto da população passará ao menos uma hora conectada por dia em um metaverso para trabalho, compras, educação, mídia social e/ou entretenimento. Nesse sentido, indica o conceito do metaverso que se busca construir:

> Um metaverso não é independente de dispositivo, nem pertence a um único fornecedor. É uma economia virtual independente, possibilitada por moedas digitais e tokens não fungíveis (NFTs). Como uma inovação combinatória, os metaversos requerem múltiplas tecnologias e tendências para funcionar. As tendências incluem realidade virtual (VR), realidade aumentada (AR), estilos de trabalho flexíveis, head-mounted displays (HMDs), uma nuvem AR, a Internet das Coisas (IoT), 5G, inteligência artificial (AI) e computação espacial[21].

Assim, a Web3 e o metaverso complementam-se em uma comunidade ou ecossistema em que o valor de alguma forma é trocado entre pessoas ou organizações — ou uma combinação. É nesse ambiente que ferramentas IoT ganham espaço no que tange à coleta de dados pessoais, para as quais daremos o nome de *wearables* ou "vestíveis"[22]. É aqui, portanto, que se encontra a grande intersecção entre IoT e Web3, no que tange ao tratamento de dados pessoais, conforme será explorado a seguir.

21. WILES, Jackie. What Is a Metaverse? And Should You Be Buying In? *Gartner*, 21 out. 2022. Disponível em: https://www.gartner.com/en/articles/what-is-a-metaverse. Acesso em 30 mar. 2023.
22. Apesar de existir alguma discussão sobre sua classificação como dispositivos de Internet das Coisas ou não, consideramos, neste artigo, apenas aqueles que se conectam à internet.

4. IOT E METAVERSO: A PROTEÇÃO DOS DADOS PESSOAIS

Como mencionado anteriormente, *wearables* são utilizados para permitir uma maior imersão do usuário na aplicação utilizada, como ao longo de uma jornada em um jogo no metaverso. Isso porque, ao permitir a convergência de mundos virtuais e reais em um ambiente tridimensional, mundos de metaverso permitem a interação dos usuários, por meio de seus avatares, em tempo real, tornando-se valiosas fontes de informações.

As situações vividas no metaverso permitem que, além dos dados compartilhados pelos próprios usuários – nome de usuário, aparência do avatar, voz, informações trocadas, sejam inferidas informações sobre seu comportamento e preferências, como já ocorre atualmente nas redes sociais e plataformas digitais de comércio eletrônico. O objetivo da coleta de dados mencionado pelas plataformas é comum, incluindo (i) o oferecimento de um serviço personalizado; (ii) a interação com o usuário; (iii) análise da utilização da plataforma; (iv) compartilhamento das informações com outras empresas; (v) monitoramento de eventuais abusos, discriminações e outros atos ilícitos na plataforma.

Para a maioria dessas funções, os *wearables* têm papel essencial, pois melhoram a experiência do usuário e permitem a maior coleta de informações, principalmente com a exploração da tecnologia 5G. Alguns exemplos são os já mencionados óculos de realidade aumentada e headsets, que possibilitam um rastreio de toda a trajetória do usuário, assim como uma verificação dos seus interesses ou não. Também existem tecidos inteligentes que permitem trocas sensoriais durante alguma interação no universo digital, como uma espécie de plástico com milhões de dispositivos magnéticos conectados para permitir que o indivíduo sinta o que ocorre com seu avatar. Além disso, empresas como Vnntr Cybernetics se empenham em desenvolver maneiras de o usuário sentir cheiros por meio da experiência digital.

Portanto, a quantidade de dados pessoais coletados no ambiente *online*, que já era extensa, ganha uma lista de infinitas possibilidades com o uso de *wearables*. Apenas a título de exemplificação, destaca-se pesquisa de dois cientistas australianos sobre o tema[23], na qual demonstraram que em vinte minutos de utilização de óculos de

23. VENTURA, Ivan. Metaverso: a fome insaciável por dados dos óculos de realidade virtual.

realidade virtual seria possível coletar dois milhões de informações relacionadas a movimentos corporais, como movimento dos olhos, dilatação de pupilas, batimento cardíaco etc.

Diante desse contexto, existem pontos de atenção às empresas que pretendem usufruir da coleta massiva de informações. A primeira delas refere-se à aplicação extraterritorial de regulamentos e leis de proteção de dados pessoais, vez que essas plataformas muitas vezes não estão localizadas no país da empresa. Como simples exemplo, uma empresa brasileira pode se sujeitar ao Regulamento Geral de Proteção de Dados da União Europeia (GDPR) caso ofereça bens ou serviços para residentes da União Europeia (conforme artigo 3º do referido regulamento).

Alguns princípios também são comuns em matéria de proteção de dados pessoais, como a importância de manter as atividades de modo transparente, o que deve ocorrer por meio de Avisos de Privacidade claros, coesos e acessíveis aos usuários. Nesses Avisos, a finalidade do tratamento deve ser informada ao titular, incluindo eventuais compartilhamentos de dados entre empresas. Por exemplo, a empresa proprietária do sistema de um *wearable* poderá usar dados pessoais que demonstram o interesse do usuário por determinado produto no metaverso e enviar essa informação para a empresa responsável pela venda desses produtos? Ou, de outro lado, a plataforma de metaverso, caso ainda não seja descentralizada, poderá compartilhar informações do usuário com terceiros interessados ou para direcionar seu próprio conteúdo ou demais serviços?

A coleta de apenas dados pessoais necessários para atingir determinada finalidade é polêmica, pois empresas desejam ter acesso a todos e quaisquer dados pessoais visando à personalização de produtos e serviços, com o posterior direcionamento de conteúdo. Esse princípio, ao ver dos autores, é um dos mais complexos a ser respeitado no ambiente digital. Por fim, também se destacam os princípios da não discriminação abusiva ou ilícita, da segurança e prevenção, além da prestação de contas.

Ainda tanto as plataformas de metaverso, como empresas responsáveis pelo gerenciamento dos *wearables* deverão ter medidas de segurança, técnicas e administrativas, aptas a protegerem a massiva quantidade de dados pessoais que será

Consumidor Moderno, 09 jun. 2022. Disponível em https://www.consumidormoderno.com.br/2022/06/09/metaverso-dados-realidade-virtual/. Acesso em 01 abr. 2023.

armazenada durante e após a utilização do sistema pelo usuário.

A proteção dos dados pessoais de crianças e adolescentes também ganha relevância, diante da grande quantidade de usuários do metaverso nessa faixa etária[24]. Em tal contexto, o tratamento deve ser informado a pais e responsáveis, algumas vezes exigindo seu consentimento, além de ter uma linguagem clara para referidos titulares menores de idade. Vale mencionar que a LGPD, por exemplo, traz, em seu artigo 14, §4º, a obrigação de controladores não condicionarem a participação dos titulares em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais, como a utilização do metaverso, além das estritamente necessárias à atividade. Do mesmo modo, o GDPR aborda questões específicas de proteção de dados pessoais de crianças e adolescentes.

Não menos importante, agentes de tratamento devem se certificar da existência de uma hipótese legal autorizativa para cada uma das operações realizadas envolvendo dados pessoais e permitir que titulares solicitem o exercício de seu direito por canal de fácil acesso. Este, idealmente, deve estar disponível no Aviso de Privacidade.

Portanto, sem intuito de esgotar as questões relativas à proteção de dados pessoais nesse ambiente digital, é certa a necessidade de um olhar atento para garantir a proteção desse direito fundamental. Por fim, outras regulamentações também tangenciam o assunto e devem ser consideradas, como questões ainda em aberto sobre inteligência artificial, tecnologia 5G e plataformas digitais, além de disposições específicas para proteção do consumidor e de demais direitos fundamentais dos indivíduos.

5 CONSIDERAÇÕES FINAIS

O comportamento do homem molda a tecnologia e a tecnologia molda o comportamento do homem, sendo, ambos, fatores que impulsionam o desenvolvimento econômico e alterações sociais. A IoT já fez alguns aniversários e sustenta a promessa de conectar dispositivos à internet e facilitar o dia a dia dos indivíduos. Essa

24. BARROS, Walter. Jovens esperam passar mais tempo em jogos do metaverso, revela pesquisa. *Cointelegraph*, 12 set. 2022. Disponível em https://cointelegraph.com.br/news/youngsters-expect-to-spend-more-time-in-metaverse-games-research-reveals. Acesso em 01 abr. 2023.

tecnologia tem sido explorada também nos *wearables*, ferramentas "vestíveis" que permitem que o usuário tenha experiências cada vez mais imersivas.

Um dos ambientes que permite essa junção de conectividade e imersão são as plataformas de metaverso, nas quais usuários têm acesso a shows, eventos, exposições de arte, além de terem um espaço de convívio social e, inclusive, trabalho. Com esses vestíveis, como óculos de realidade virtual, os mundos de metaverso se tornam até mesmo palpáveis aos quatro sentidos.

Contudo, como ocorre com o advento de qualquer nova tecnologia, surgem também desafios jurídicos. Um deles, abordado neste artigo, é a proteção dos dados pessoais dos usuários, cuja coleta se torna ainda mais intensa diante da utilização de vestíveis neste ambiente imersivo. As possibilidades de exploração econômica são muitas, indo desde o direcionamento de conteúdo e publicidade comportamental, até a modulação de inteligência artificial. Este desenvolvimento deve ser acompanhado de medidas éticas, ferramentas que garantam transparência e protejam direitos fundamentais.

Além da legislação existente, também se discute a regulamentação de plataformas digitais no país e o tema já avançou de modo relevante na União Europeia, por meio do Digital Markets Act e do Digital Services Act. No entanto, algumas questões estão em aberto e devem ser urgentemente endereçadas para evitar riscos aos usuários, inclusive a crianças e adolescentes, que são o público majoritário dessa tecnologia.

Assim, é importante (re)pensar a arquitetura jurídica digital, não apenas a nível de legislação propriamente dito, mas de regulação e políticas públicas. Obviamente que diante de constante evoluções e novas situações que demandam sempre novas arquiteturas, há uma grande dificuldade que se depreende ínsita. Exatamente diante desta dificuldade que o Direito deve buscar soluções "fora da caixa", inventivas, criativas, utilizando-se das próprias "armas" utilizadas para a "criação" de novas invenções tecnológicas.

REFERÊNCIAS

BARROS, Walter. Jovens esperam passar mais tempo em jogos do metaverso, revela pesquisa. *Cointelegraph*, 12 set. 2022. Disponível em https://cointelegraph.com.br/news/youngsters-expect-to-spend-more-time-in-metaverse-games-research-reveals. Acesso em 01 abr. 2023.

BASSI, A.; HORN, G. Internet of Things in 2020: A Roadmap for the Future. European Commission: *Information Society and Media*, v. 22, p. 97-114, 2008. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://docbox.etsi.org/erm/Open/CERP%2020080609-10/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v1-1.pdf. Acesso em: 27 mar. 2023.

BLOCKCHAIN CONCIL. *How Will IoT Integrate The Real World With The Metaverse*? Set., 2022. Disponível em: https://www.blockchain-council.org/metaverse/how-will-iot-integrate-the-real-world-with-the-metaverse/#:~:text=The%20combination%20of%20Metaverse%20and,virtual%20experiences%20to%20its%20users. Acesso em: 25 mar. 2023.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil*: Consulta Pública. Dez. 2016. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.abinee.org.br/informac/arquivos/aiot.pdf. Acesso em: 26 mar. 2023.

BRASIL. Decreto nº 9.854, de 25 de junho de 2019. *Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas*. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm#art10. Acesso em: 25 mar. 2023.

BRASIL. Lei 13.709 de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 mar. 2023.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Consulta pública*: Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil, dez. 2016.

CASTELLS, Manuel. *A sociedade em rede*. 8.ed. v. 1. Trad. Roneide Venancio Majer. São Paulo: Paz e Terra, 1999. P

CENDÃO, Fábio; ANDRADE, Lia. *Direito, metaverso e NFTs*: introdução aos desafios na web3. São Paulo: ExpressaJur, 2022.

DOMINGUES, Juliana Oliveira; MIELE, Aluísio de Freitas; QUINELATO, Pietra Daneluzzi; HERNANDES, Beatriz; RAFIH, Rhasmye El. *Fashion Law*: o direito está na moda. São Paulo: Singular, 2019.

FALEIROS JR., José Luiz de Moura. Responsabilidade por falhas de algoritmos de inteligência artificial: ainda distantes da singularidade tecnológica, precisamos de marcos regulatórios para o tema? *Revista de Direito da Responsabilidade*, ano 4, 2022. Disponível em: https://www.academia.edu/88822610/Responsabilidade_por_falhas_de_algoritmos_de_intelig%C3%AAncia_artificial_ainda_distantes_da_singularidade_tecnol%C3%B3gica_precisamos_de_marcos_regulat%C3%B3rios_para_o_tema. Acesso em 20 mar. 2023.

KENNEDY, John B. *When Woman is boss*. 30/01/1926. Disponível em:

https://teslauniverse.com/nikola-tesla/articles/when-woman-boss. Acesso em: 27 mar. 2023.

MAGRANI, Eduardo. *A internet das Coisas*. São Paulo: Editora FGV, 2018. Disponível em: Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 26 mar. 2023.

VENTURA, Ivan. Metaverso: a fome insaciável por dados dos óculos de realidade virtual. *Consumidor Moderno*, 09 jun. 2022. Disponível em https://www.consumidormoderno.com.br/2022/06/09/metaverso-dados-realidade-virtual/. Acesso em 01 abr. 2023.

WILES, Jackie. What Is a Metaverse? And Should You Be Buying In? *Gartner*, 21 out. 2022. Disponível em: https://www.gartner.com/en/articles/what-is-a-metaverse. Acesso em 30 mar. 2023.

HOLOGRAMAS NA INTERNET DAS COISAS

José Luiz de Moura Faleiros Júnior

Doutorando em Direito, na área de estudo 'Direito, Tecnologia e Inovação', pela Universidade Federal de Minas Gerais. Doutorando em Direito Civil pela Universidade de São Paulo. Mestre e Bacharel em Direito pela Universidade Federal de Uberlândia. Especialista em Direito Digital. Advogado. Professor. Contato: jfaleiros@ufmg.br

Lucas Enriquez Rocha

Graduado em Direito pela Faculdade de Direito da Universidade de São Paulo – USP/Largo de São Francisco. Participante de duas edições consecutivas do BRICS International School (2020 e 2021), programa científico internacional voltado para pesquisadores e estudantes dos países-membros do BRICS (Brasil, Rússia, Índia, China e África do Sul). Desenvolve pesquisa sobre os impactos da tecnologia 5G quanto ao direito à privacidade no contexto brasileiro. Contato: lucas.ler@alumni.usp.br

DOI: https://doi.org/10.59224/dti5.ch17

Resumo: Neste artigo, são discutidos os desafios éticos e jurídicos associados à fabricação e uso de hologramas, bem como as implicações para a sociedade. A tecnologia dos hologramas oferece novas formas de comunicação e interação com o mundo, mas também apresenta riscos e desafios para a privacidade e a segurança de dados, especialmente em relação à coleta e ao uso de dados pessoais sensíveis. Este artigo também destaca a necessidade de preparar a Ciência Jurídica para lidar com as questões jurídicas e éticas relacionadas aos hologramas. As implicações dos hologramas para a segurança nacional e a cibersegurança são analisadas, examinando-se os desafios de proteger dados e informações sensíveis em um ambiente cada vez mais complexo e interconectado. As oportunidades e desafios de usar essa tecnologia para promover a

***Abstract: In** this article, the ethical and legal challenges associated with the manufacturing and use of holograms, as well as the implications for society, are discussed. Hologram technology offers new ways of communicating and interacting with the world, but also presents risks and challenges to privacy and data security, especially regarding the collection and use of sensitive personal data. This article also highlights the need to prepare legal science to deal with the legal and ethical issues related to holograms. The implications of holograms for national security and cybersecurity are analyzed, examining the challenges of protecting sensitive data and information in an increasingly complex and interconnected environment. The opportunities and challenges of using this technology to promote*

transparência, a participação cívica e a prestação de serviços públicos mais eficientes e acessíveis no contexto da Internet das Coisas (IdC) também são examinados. A metodologia utilizada para esta investigação é dedutiva, com base em pesquisa bibliográfica e qualitativa.

Palavras-chave: holografias; privacidade; Internet das Coisas; segurança de dados; regulação.

transparency, civic participation, and more efficient and accessible public services in the context of the Internet of Things (IoT) are also examined. The methodology used for this investigation is deductive, based on bibliographic and qualitative research.

Keywords: *holograms; privacy; Internet of Things; data security; regulation.*

1. INTRODUÇÃO

A tecnologia dos hologramas está cada vez mais presente na sociedade contemporânea, oferecendo novas formas de comunicação e interação com o mundo. No entanto, essa tecnologia também traz consigo novos desafios e riscos, especialmente em termos de privacidade e segurança de dados quando são utilizados dispositivos diretamente conectados, dando ensejo à chamada Internet das Coisas (IdC, ou *Internet of Things*, IoT). Neste artigo, serão debatidos alguns dos desafios jurídicos e éticos associados à fabricação e ao uso de hologramas, bem como as implicações para a sociedade como um todo.

De início, será examinado o estado atual da regulamentação dos hologramas ao redor do mundo, incluindo as iniciativas em curso para estabelecer diretrizes e normas para a fabricação e uso dessas tecnologias. Em seguida, serão abordados alguns desafios éticos e de proteção à privacidade associados aos hologramas, especialmente em relação à coleta e uso de dados pessoais sensíveis. Serão analisadas as implicações dessas tecnologias para a privacidade, para a intimidade e para a preservação da imagem.

Outro tema importante que será explorado neste artigo é a necessidade de preparar a Ciência Jurídica para lidar com as questões jurídicas e éticas relacionadas aos hologramas. Em seguida, serão analisadas as implicações dos hologramas para a

segurança nacional e a cibersegurança, examinando os desafios de proteger dados e informações sensíveis em um ambiente cada vez mais complexo e interconectado, inclusive em relação às políticas públicas e à governança, examinando as oportunidades e desafios de usar essa tecnologia para promover a transparência, a participação cívica e a prestação de serviços públicos mais eficientes e acessíveis no contexto da Internet das Coisas (IdC).

Destaca-se que a metodologia utilizada para esta investigação é dedutiva, com base em pesquisa bibliográfica e qualitativa.

2. HOLOGRAMAS COMO PRINCIPAL MEIO DE COMUNICAÇÃO DO FUTURO

Sempre que uma nova tecnologia surge, indaga-se se ela trará benefícios sem precedentes ou se levará ao caos, à piora na qualidade de vida e aos conflitos[1]. É importante considerar que invenções tecnológicas são uma "faca de dois gumes". A energia nuclear, por exemplo, levou a muitos avanços, mas também resultou em tragédias, como as bombas de Hiroshima e Nagasaki. A pólvora, por sua vez, foi usada para criar fogos de artifício, mas também foi utilizada para desenvolver as primeiras armas de fogo.

Via de regra, o implemento da transformação em sociedade, seja por eventos históricos ou mesmo pelo implemento de novas tecnologias, tem o condão de romper um paradigma dominante e ressignificar a ciência. Nos dizeres de Boaventura de Sousa Santos, "o conhecimento científico avança pela observação descomprometida e livre, sistemática e tanto quanto possível rigorosa dos fenómenos naturais"[2]. Logo, é papel do cientista indagar quais são os reflexos mediatos de uma transformação que

1. Com efeito: "Alguns teóricos argumentam que o efeito geral desses processos globais tem sido o de enfraquecer ou solapar formas nacionais de identidade cultural. Eles argumentam que existem evidências de um afrouxamento de fortes identificações com a cultura nacional, e um reforçamento de outros laços e lealdades culturais, (...)". HALL, Stuart. *A identidade cultural na pós-modernidade*. Tradução de Tomaz Tadeu da Silva e Guacira Lopes Louro. Rio de Janeiro: DP&A, 1997, p. 73.
2. SANTOS, Boaventura de Sousa. *Um discurso sobre as ciências*. Porto: Edições Afrontamento, 1997, p. 13.

se sofistica e que desencadeia múltiplos fenômenos[3].

Ao aplicar esse questionamento específico aos hologramas, surge a seguinte questão: esta nova tecnologia será uma dádiva ou um flagelo, um Fogo de Prometeu ou uma Caixa de Pandora?[4] Conceitualmente, o holograma nada mais é que uma imagem tridimensional gerada por difração e interferência de feixes de luz, usando tecnologia a laser que está disponível desde os anos 60. No entanto, a velocidade de transmissão de dados insuficiente impediu a interconexão dos elementos necessários para torná-lo viável. Com a chegada do 6G, a sexta geração de comunicação sem fio, essa limitação será superada, possibilitando uma conexão mais rápida, estável, larga e com menor latência[5].

3. Sobre tal mister, valioso o questionamento de Einstein: "Qual a meta que deveríamos escolher para nossos esforços? Será o conhecimento da verdade ou, em termos mais modestos, a compreensão do mundo experimental, graças ao pensamento lógico coerente e construtivo? (...) O esforço para o conhecimento, por sua própria natureza, nos impele ao mesmo tempo para a compreensão da extrema variedade da experiência e para o domínio da simplicidade econômica das hipóteses fundamentais". EINSTEIN, Albert. *Como vejo o mundo*. Tradução de H.P. de Andrade. Rio de Janeiro: Nova Fronteira, 2011, p. 197-198.
4. De acordo com a lenda da Grécia Antiga, os deuses do Olimpo criaram várias raças de seres vivos para habitarem a Terra, incluindo animais e humanos. Para essa tarefa, dois titãs, os irmãos Prometeu e Epimeteu, foram chamados pelas entidades divinas: Epimeteu ficaria responsável pela criação e Prometeu supervisionaria o processo. No entanto, Epimeteu percebeu que os humanos seriam fracos em comparação com as outras criações. Compadecido, Prometeu roubou o Fogo pertencente à Héstia, deusa dos lares, da família e da lareira, e o entregou à humanidade. Com o Fogo, os humanos ganharam esperteza, sagacidade, coragem e ímpeto, tornando-se mais poderosos que os animais. Por medo do potencial dos humanos, Zeus, o maior dos deuses, puniu Prometeu, acorrentando-o no topo de uma montanha, onde ele seria devorado todos os dias por uma águia que comia seu fígado. Para piorar a situação, Zeus criou Pandora, a primeira mulher, e ofereceu-a como esposa para Epimeteu, junto com uma caixa que não deveria ser aberta. Pandora, movida pela curiosidade insaciável, abriu a caixa, libertando todos os males para a humanidade, deixando apenas a esperança. BURKERT, Walter. *Greek Religion*: Archaic and Classical. Oxford: Blackwell Publishing, 1991, p. 139-141.
5. ACKERMANN, Gerhard K.; EICHLER, Jürgen. *Holography*: a practical approach. Cham: Springer, 2007, p. 1. Definem: "Basic holography consists of the production of a hologram, which is a photographic recording of the pattern of interference created when coherent light reflected from or transmitted through an object is superimposed with a reference beam of the same frequency. When the hologram is illuminated with a beam of light identical in frequency and angle

Os hologramas têm o potencial de substituir os dispositivos de comunicação atuais, como telefones, televisores e computadores, e oferecer uma experiência de comunicação mais natural e imersiva[6], permitindo a transmissão de imagens em 3D que emulam perfeitamente uma pessoa em sua totalidade, expondo gestos, olhares, expressões faciais e reações emocionais com mais clareza e rapidez[7]. Além disso, com a integração coordenada de outros dispositivos próximos, como emissores de áudio, é possível criar uma forma de interação baseada nos sentidos humanos, como a comunicação háptica, que se baseia no tato. Essas características representam um grande avanço qualitativo em comparação às telas usadas atualmente, pois reduzem a dependência das mesmas e possibilitam novas formas de interação à distância.

A importância dos hologramas no campo da comunicação nos próximos 10 a 15 anos se destaca pela necessidade de analisar os dilemas relacionados ao direito à privacidade, que serão intensamente afetados por essa nova tecnologia. Até então, a comunicação à distância tem sido dominada por telefones fixos, móveis, *smartphones* e computadores com telas. Com o advento do holograma, esses artefatos se tornarão obsoletos, dando lugar à telecomunicação holográfica[8].

Os hologramas não apenas substituirão os dispositivos atuais, como também melhorarão a qualidade e variedade dos serviços oferecidos. Com a alta velocidade de dados e menor latência do 6G, os hologramas permitirão uma comunicação mais natural e ampla[9], em que as imagens transmitidas em 3D poderão emular

---

of incidence as the reference beam, the original object appears to float in space at a location behind the hologram. This is an important feature of holograms, as it provides the viewer with a true three-dimensional representation of the object".

6. SILVA, Ana Carolina S.; OLIVEIRA, Eliane R. O Uso de Hologramas na Comunicação: Benefícios e Preocupações com a Privacidade. *Revista Brasileira de Marketing*, São Paulo, v. 19, n. 3, p. 142-152, 2020, p. 143-144.
7. KOBAYASHI, Yutaka. Holographic technology for practical 3D displays. *Proceedings of the IEEE*, [S.l], v. 102, n. 2, p. 187-201, 2014.
8. ANDERSON, Cristopher W. *et al.* Legal and ethical implications of the use of holographic and augmented reality technologies for education and training. In: *ASEE Annual Conference & Exposition*, 2019. Proceedings. Tampa, FL: American Society for Engineering Education, 2019. p. 15.
9. Valioso, nesse ponto, o pensamento de Talbot: "Although the brain does indeed act like a hologram, it is not a hologram. Rather, it is a holographic projector. When we see a tree, our brain does not reconstruct the tree from bits and pieces of information like a jigsaw puzzle. Instead, it projects

perfeitamente uma pessoa em sua totalidade, com gestos, olhares, expressões faciais e reações emocionais[10]. Além disso, a comunicação háptica poderá ser estabelecida, criando hologramas táteis que podem ser tocados e sentidos[11].

Essas características representarão um grande avanço em relação às telas atuais, que cansam o cérebro e a visão e exigem mais energia para a comunicação sem elementos de interação não verbal. Os hologramas ocuparão de forma massiva o espaço atualmente reservado aos aparelhos, reunindo e melhorando todos seus pontos positivos, trazendo benefícios à humanidade, como maior flexibilidade de comunicação, novas formas de interação à distância e redução de riscos em atividades perigosas[12].

No entanto, é importante considerar os riscos à privacidade e outros problemas relacionados que serão amplificados com a interação holográfica. Esses riscos já existem na geração atual de telecomunicações, mas serão aumentados com a utilização do holograma.

---

the entire tree outside our head and we see it 'out there' in the world". TALBOT, Michael. *The Holographic Universe*: the revolutionary theory of reality. Nova York: HarperPerennial, 2011, p. 48.

10. Com efeito: "Holographic communication will allow us to see and interact with remote individuals and objects as if they were present in our own space. Holography uses the principle of diffraction to record the light field emanating from an object, and to reconstruct the light field at a later time, using only light. The holographic system records the amplitude and phase of the wave fronts of the object light field. These amplitude and phase components are recorded onto a photosensitive medium, where they interfere with a reference beam to form a hologram. When the hologram is illuminated with a coherent light source, the original wave front is reconstructed, yielding a three-dimensional (3D) image of the object. Holographic communication requires a high bandwidth to transmit the amplitude and phase components of the object light field, which makes it an attractive application for the upcoming 5G and 6G communication networks". AMIN, Muhammad Bilal *et al*. HoloLens: Enabling Technology for Future Communication Networks. *IEEE Communications Magazine*, [S.l], v. 55, n. 3, p. 154-161, mar. 2017, p. 158.
11. HUANG, Keping; YAN, Li. Holographic Communications: A State-of-the-Art Review. *IEEE Communications Magazine*, v. 58, n. 4, p. 15-21, 2020, p. 16.
12. KIM, Yuna *et al*. HoloPrivacy: Enabling Privacy in Holographic Communication. In: *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018. p. 1-6.

3. PREOCUPAÇÕES ÉTICAS E JURÍDICAS RELACIONADAS AOS HOLOGRAMAS

O uso de hologramas como meio de comunicação trará muitos benefícios, mas também algumas preocupações, principalmente em relação à privacidade. Primeiramente, os hologramas podem ser usados para invadir a privacidade das pessoas, pois eles possibilitam a criação de imagens e vídeos em 3D muito realistas, que podem ser facilmente manipulados e divulgados sem o consentimento do indivíduo[13]. Isso pode levar à prática de crimes de assédio, extorsão e falsidade ideológica, além de outras formas de violação da privacidade, com consequências variadas.

Além disso, os hologramas permitem a coleta de dados pessoais de maneira ainda mais invasiva do que os dispositivos atuais, já que podem capturar imagens em 3D e até mesmo informações hápticas. Isso significa que as empresas de telecomunicações e outras organizações terão acesso a dados muito mais detalhados sobre os indivíduos, o que pode ser usado para fins de publicidade e marketing, mas também para espionagem e vigilância.

Outra preocupação é que os hologramas possam ser usados para falsificar identidades, já que podem criar imagens e vídeos muito realistas de uma pessoa[14]. Isso pode levar a casos de fraudes e roubos de identidade, bem como a uma maior dificuldade na verificação da autenticidade de informações e comunicações[15]. Isso pode ser particularmente problemático em áreas como a segurança nacional e a justiça, nas quais a veracidade das informações é crucial.

Além disso, a comunicação holográfica pode permitir a criação de espaços virtuais compartilhados, onde várias pessoas podem interagir em um ambiente virtual tridimensional. Embora isso possa ser uma vantagem em muitos aspectos, também cria

13. MACEDO, Francisco Alves de. Comunicação holográfica e privacidade: Desafios e perspectivas. In: *Anais do III Encontro de Tecnologia da Informação e Comunicação (ETIC)*, Natal, RN, Brasil, 2019. p. 1-10.
14. BARCELLOS, Ekaterina; MERCALDI, Marlon; PINHEIRO, Olympio; BOTURA JR., Galdenoro. Holografia: inovação e metáfora de interatividade na comunicação e na representação ótica. In: *Anais do 7º Congresso Internacional de Design da Informação*. São Paulo: Blucher, 2015, p. 579-580.
15. KIM, Yuna *et al.* HoloPrivacy: Enabling Privacy in Holographic Communication. In: *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018. p. 1-6.

riscos de violação da privacidade, especialmente se as informações e comunicações nesses espaços não forem devidamente protegidas. Isso pode levar a casos de espionagem industrial, roubo de propriedade intelectual e outras formas de violação da privacidade.

Por fim, a comunicação holográfica também trará desafios em relação à segurança cibernética, pois os hologramas estarão conectados à Internet e serão vulneráveis a ataques cibernéticos e outras formas de intrusão[16]. Isso pode levar a incidentes de segurança com dados pessoais, interrupções no serviço e outras consequências negativas. É essencial que as empresas de telecomunicações e outras organizações tomem medidas adequadas para proteger a privacidade e a segurança dos usuários de comunicação holográfica, a fim de minimizar esses riscos[17].

Com a maior velocidade do tráfego de dados e as frequências mais altas, o número dos equipamentos necessários para a transmissão e retransmissão será cada vez maior, devido ao fato de que, de acordo com as leis da Física, quanto maior a frequência da onda, menor a altura desta[18]. Por conseguinte, o alcance de cada onda da radiação será de grau mais reduzido, levando à necessidade de implementação de mais equipamentos em cada área geográfica, para suprir tal distância física, aparatos estes que, pela alta densidade, deverão ser cada vez menores.

Existem várias iniciativas globais voltadas ao desenvolvimento de hologramas para diversas aplicações, desde entretenimento até saúde e educação[19]. Algumas das principais são:

(i) *Microsoft HoloLens*: A empresa norte-americana Microsoft desenvolveu o

16. KOZAK, Radoslaw; ZOLICH, Artur; URBAN, Grzegorz. Security issues in IoT-based devices. *Journal of Cybersecurity*, Oxford, v. 4, n. 1, p. 1-17, 2018, p. 10-13.
17. LIEBIG, Tobias; DIETRICH, Daniel; JUNG, Peter. HoloSec: Towards Secure and Privacy-Preserving Holographic Videoconferencing. In: *Proceedings of the 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, p. 1-6.
18. KOWALCZYK, Tomasz; WEGNER, Krzysztof. Privacy and Security Aspects of Holographic Communication Systems. In: *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Prague, Czech Republic, 2017, p. 1033-1040.
19. Cf. GIACOMINI, Michele; ZANNONI, Michele. Hologram technology: a review of recent development in optics, photonics and nanotechnologies. *Micro & Nano Letters*, [S.l], v. 15, n. 12, p. 982-986, 2020. Disponível em: https://doi.org/10.1049/mnl2.2020.0231. Acesso em: 04 mar. 2023.

HoloLens, um *headset* de realidade aumentada que projeta imagens holográficas em tempo real. O dispositivo tem aplicações em treinamento, manufatura, design, saúde e educação[20];

(ii) *Magic Leap*: A empresa americana Magic Leap desenvolveu uma tecnologia de realidade aumentada que projeta imagens holográficas em ambientes reais. Seus dispositivos têm aplicações em jogos, entretenimento, educação e negócios[21];

(iii) *Holovis*: A empresa britânica Holovis é especializada em tecnologia holográfica para entretenimento e parques temáticos que criam experiências imersivas em 3D usando projeções holográficas em telas ou espaços vazios[22];

(iv) *HoloPundits*: A empresa norte-americana HoloPundits desenvolve tecnologia holográfica para treinamento, educação e negócios. Hologramas são utilizados para criar ambientes virtuais em 3D para simulações e treinamento[23];

(v) *Light Field Lab*: A empresa norte-americana Light Field Lab está desenvolvendo *displays* holográficos volumétricos em escala real, que podem exibir imagens holográficas em 3D sem a necessidade de óculos especiais com aplicações em entretenimento, publicidade e arquitetura[24];

(vi) *Leia Inc.*: A empresa norte-americana Leia Inc. desenvolveu uma tecnologia de exibição de imagens holográficas usando um *display* de luz difusa. Seus dispositivos têm aplicações em entretenimento, publicidade, educação e saúde[25].

Essas iniciativas representam apenas uma amostra do desenvolvimento de tecnologia holográfica atualmente em andamento em todo o mundo, mas o que isso

20. MICROSOFT. *HoloLens*. Disponível em: https://www.microsoft.com/pt-br/hololens. Acesso em: 04 mar. 2023.
21. MAGIC LEAP. *Magic Leap One*. Disponível em: https://www.magicleap.com/magic-leap-one. Acesso em: 04 mar. 2023.
22. HOLOVIS. *Holovis - What We Do*. Disponível em: https://holovis.com/what-we-do/. Acesso em: 04 mar. 2023.
23. HOLOPUNDITS. *Holopundits - What We Do*. Disponível em: https://www.holopundits.com/what-we-do/. Acesso em: 04 mar. 2023.
24. LIGHT FIELD LAB. *Light Field Lab - What We Do*. Disponível em: https://www.lightfieldlab.com/what-we-do. Acesso em: 04 mar. 2023.
25. LEIA INC. *Leia's Display*. Disponível em: https://www.leiainc.com/technology/. Acesso em: 04 mar. 2023.

implicará para a privacidade? Basicamente, por meio do maior número de equipamentos e a capacidade de transmissão de dados muito mais ampla, tornar-se-á possível uma maior e mais numerosa participação de distintos atores na comunicação holográfica. Isto é, uma quantidade muito maior de pessoas diferentes, com interesses diversos, participando de uma mesma comunicação, e mais: com abundância informacional inimaginável![26]

Para visualizar tal caso com mais concretude, imagine-se o seguinte cenário: uma pessoa está se comunicando com outra pelo holograma, e decide fazer uma reunião com outros colegas. Os vários equipamentos permitirão que um montante altíssimo de membros seja inserido nessa conversa[27].

A possibilidade de integração de vários elementos para que o holograma funcione é outro ponto a ser considerado. Isso porque será necessário um equipamento para a transmissão e produção de imagem, outro para a emissão de voz, um terceiro para captar gestos, além de outro para capturar expressões faciais, entre outros. Essa necessidade implica que cada aspecto e equipamento exigirá uma empresa diferente, altamente especializada no assunto. Essa hiperespecialização será indispensável, já que no contexto de interação por holograma, é crucial que haja coordenação minuciosa em todos os detalhes, inclusive no nível dos circuitos dos *chips* eletrônicos.

Como evitar que terceiros mal-intencionados explorem as possíveis falhas de segurança em um dos equipamentos de várias empresas diferentes, para obter dados

26. Segundo Michael Talbot: "In the holographic model, every place in the universe contains all the information in the universe, and every piece of holographic film, no matter how small, contains all the information of the universe. This means that if a holographic film were cut in half and then illuminated with a laser, each half would still contain all the information of the whole. If each of these halves were cut in half, each of the resulting quarters would contain all the information of the whole as well. In other words, the information in the universe is distributed in such a way that every part of the universe contains all the information of the whole, but on a smaller scale". TALBOT, Michael. *The Holographic Universe*: the revolutionary theory of reality. Nova York: Harper-Perennial, 2011, p. 16.

27. LAAROUSSI, Zakaria; SOYKAN, Elif Ustundag; LILJENSTAM, Michael; GULEN, Utku; KARAÇAY, Leyli; TOMUR Emrah. On the security of 6G use cases: Threat Analysis of "All-Senses Meeting". *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, 8 a 11 de Janeiro de 2022. Disponível em: https://ieeexplore.ieee.org/document/9700673. Acesso em: 04 mar. 2023.

de conversas realizadas por hologramas, em um cenário de troca de dados extremamente rápida?[28] E se uma das empresas compartilhar indevidamente esses dados com outras partes, o que será feito? Com várias empresas trabalhando simultaneamente, múltiplos equipamentos e alta velocidade de troca de dados, é difícil imaginar como um sistema de vigilância e segurança poderá ser efetivamente aplicado. Além disso, surge a questão da responsabilização em caso de descoberta de falhas de segurança[29]. Com o uso de hologramas, é necessário um nível de coordenação sem precedentes entre diferentes operadoras. Será possível identificar a empresa responsável pelo vazamento de informações em meio a esse encadeamento e integração de várias companhias?

É possível notar, portanto, um triplo risco decorrente da comunicação holográfica: o risco de múltiplas pessoas conversando simultaneamente, o risco do grande número de equipamentos e empresas atuando ao mesmo tempo e a dificuldade em identificar o responsável por uma eventual falha (e do subsequente ilícito gerador de dano). E, embora já existam alguns dispositivos de exibição de hologramas

28. Denotando tal preocupação, cita-se a reflexão de Lane Thames e Emily Miller: "The underlying technologies enabling Industry 4.0, including IoT, AI, and cloud computing, are making manufacturing systems more complex and interconnected, which poses new security risks. One example of this complexity is the distributed nature of Industry 4.0 systems. Rather than relying on a single central processing unit (CPU) to manage all data processing, Industry 4.0 devices use multiple CPUs located across the system. This means that data is constantly being transmitted across the network, making it more vulnerable to interception by hackers. Additionally, the increased use of wireless communication technologies and the Internet have also made Industry 4.0 devices more susceptible to cyberattacks". THAMES, Lane; MILLER, Emily. *Cybersecurity for Industry 4.0*: analysis for design and manufacturing. Nova York: Apress, 2020. p. 40.

29. Com efeito: "As IoT devices proliferate in society, they are collecting more and more personal data that can be used to make people's lives easier, but also to track and monitor their behavior. This poses a significant privacy risk, as the aggregation of data from multiple devices can reveal sensitive personal information about individuals, such as their location, habits, and preferences. Additionally, many IoT devices are vulnerable to security breaches, which can allow hackers to gain access to private information, take control of devices, or use them as part of a larger botnet for malicious purposes. As such, it is crucial that IoT devices are designed with security and privacy in mind from the outset, and that users are educated about the risks and best practices for using these devices safely". FELICI, Massimo; PEARSON, Siani. *The Internet of Things*: Security and Privacy Issues. Cham: Springer, 2019. p. 18.

disponíveis no mercado, eles ainda não estão amplamente disponíveis para os consumidores comuns. Atualmente, a produção de hologramas em massa ainda é cara, assim como os dispositivos necessários para exibi-los. Além disso, a tecnologia de hologramas está em constante desenvolvimento e aprimoramento, o que significa que ainda há muito a ser feito para melhorar sua qualidade e torná-los mais acessíveis ao público em geral.

A tecnologia de hologramas está evoluindo rapidamente e sua demanda vem aumentando em áreas como medicina, indústria automotiva e entretenimento, o que indica uma possibilidade de tornar-se mais acessível ao mercado de consumo no futuro. No entanto, um desafio adicional que precisa ser considerado diz respeito à privacidade em relação aos hologramas, já que eles farão parte da Internet das Coisas (IdC)[30], um ecossistema de dispositivos conectados habilitados pelo 5G e, posteriormente, pelo 6G[31].

Com inúmeros aparelhos interconectados aos hologramas, os riscos de privacidade mencionados anteriormente podem ser exponencialmente ampliados. Ainda que seja possível mitigar os riscos de privacidade em empresas e equipamentos que lidam com hologramas, como lidar com outras áreas? Por exemplo, se um holograma é usado em uma cirurgia médica remota e precisa acessar dados de um equipamento hospitalar interno, o que impediria o compartilhamento desses dados com terceiros, como operadoras de planos de saúde? Outro exemplo seria um holograma que se comunica com outro dentro de um carro. Como garantir que a empresa proprietária do veículo não intercepte a conversa e obtenha informações confidenciais?

As consequências de violações de privacidade de hologramas poderiam ser ainda mais graves, incluindo informações altamente confidenciais relacionadas à segurança nacional, segredos industriais de tecnologias de última geração, diálogos entre altas autoridades políticas e trocas diplomáticas. Por exemplo, como impedir que a conversa secreta de um chefe de Estado, realizada por holograma, seja capturada por

30. Cf. KUMAR, A. Madhan; THAMPI, Sabu M. *Internet of Things*: technologies, communications and computing. Cham: Springer, 2019, *passim*.

31. GIORDANI, Marco; POLESE, Michele; MEZZAVILLA, Marco; RANGAN, Sundep; ZORZI, Michele. Towards 6G Networks: Use Cases and Technologies. *IEEE Communications Magazine*, v. 58, n. 3, mar. 2020. Disponível em: https://ieeexplore.ieee.org/document/9040264. Acesso em: 04 mar. 2023.

um dispositivo aparentemente inofensivo, como um brinquedo próximo no quarto de uma criança, e transmitida para outro dispositivo em outro país e, em seguida, para inimigos estrangeiros ou grupos terroristas?

Será necessário estabelecer formas de controle para essas interações. No entanto, surgirá um outro problema: com a alta conectividade entre diferentes dispositivos através da Internet das Coisas e sua alta velocidade, como evitar a invasão desses pontos de controle? E se invasores decidirem controlar esse acesso, impedindo a entrada ou saída do fluxo de dados de uma conversa, dependendo do caso?

Além disso, pode-se trabalhar com a hipótese de que um invasor possa assumir o controle indevido da conversa e inserir conteúdo indesejável, de diversas naturezas, no diálogo. É possível imaginar diversos cenários em que as lacunas de privacidade do holograma podem gerar problemas graves, como a captura de informações sigilosas ou a manipulação indevida de conversas[32]. Por exemplo, um invasor pode controlar o acesso a uma conversa holográfica, impedindo a entrada ou a saída da vítima. Ou ainda, um *cracker* pode gerar novos hologramas táteis para criar confusão ou até mesmo suscitar o pânico com imagens de animais perigosos.

Além disso, há a questão dos direitos autorais. Se no mundo virtual atual já se enfrenta o roubo massivo de imagens na Internet, protegidas por direitos autorais, imagine como será com os hologramas. Se uma pessoa tiver um holograma predefinido para conversas e essa imagem for replicada indevidamente, pode ser usada para ludibriar outras pessoas. Outro risco relacionado aos hologramas é a manipulação de informações por meio de *deepfakes*, que são imagens e vídeos falsos criados com sistemas de inteligência artificial baseados em *deep learning*[33]. Com essa tecnologia, mais do que a violação à imagem[34], é possível criar um holograma falso de uma

32. Para maior aprofundamento na temática dos crimes levados a efeito pela subversão tecnológica em variados contextos, inclusive pela exploração de hologramas, conferir: BARTLETT, Jamie. *The Dark Net*: inside the digital underworld. Nova York: Melville House Publishing, 2016; STRYKER, Cole. *Hacking the future*: privacy, identity, and anonymity on the web. Nova York: Overlook Press, 2012.

33. SPIVAK, Russell. "Deepfakes": The newest way to commit one of the oldest crimes. *Georgetown Law Technology Review*, Washington, DC, v. 3, n. 2, p. 339-400, 2019, p. 397.

34. Sobre o tema, comenta Filipe Medon: "Seja qual for o meio tecnológico adotado para se criar uma imagem falsa, já se pode apontar dois traços característicos, quais sejam, o emprego de técnicas

pessoa famosa, por exemplo, e fazer com que ela diga coisas que nunca disse[35]. Isso pode causar sérios danos à reputação da pessoa e até mesmo levar a consequências gravíssimas.

Além disso, os *deepfakes* também podem ser utilizados para criar situações falsas em interações holográficas, gerando uma confusão mental nas pessoas presentes e potencialmente induzindo-as a tomar decisões erradas, o que poderia até mesmo se expandir para os domínios da política[36]. É fundamental, portanto, que sejam desenvolvidas medidas de segurança para evitar a disseminação de *deepfakes* e proteger a integridade das interações por hologramas.

Com a possibilidade de criar hologramas tão realistas, é preciso levar em conta que pessoas mal-intencionadas podem utilizar essa tecnologia para criar imagens e vídeos falsos de indivíduos, a fim de difamá-los, prejudicá-los ou mesmo comprometer sua reputação. Isso pode afetar negativamente a vida pessoal e profissional dessas pessoas, além de causar danos irreparáveis à sua imagem. Ademais, a criação de hologramas implica no armazenamento e processamento de uma grande quantidade de informações, o que pode representar um risco para a privacidade das pessoas. Esses dados podem ser coletados e usados sem o consentimento dos indivíduos, o que pode violar seus direitos fundamentais à privacidade e à proteção de dados pessoais[37].

---

computacionais avançadas, comumente de inteligência artificial, assim como o grau tão elevado de realidade que faz com que seja quase impossível se detectar a fraude, o que é especialmente perigoso nos tempos atuais, marcado pela "economia da atenção". MEDON, Filipe. O direito à imagem na era das "deepfakes". *Revista Brasileira de Direito Civil - RBDCivil*, Belo Horizonte, v. 27, p. 251-277, jan./mar. 2021, p. 263.

35. DE RUITER, Adrienne. The distinct wrong of deepfakes. *Philosophy & Technology*, [S.l], v. 34, p. 1311-1332, 2021. Disponível em: https://doi.org/10.1007/s13347-021-00459-2. Acesso em: 04 mar. 2023.

36. MULHOLLAND, Caitlin; OLIVEIRA, Samuel Rodrigues. Uma nova cara para a política? Considerações sobre "deepfakes" e democracia. *Revista de Direito Público*, Brasília, v. 18, n. 99, p. 368-396, jul./set. 2021.

37. Segundo Marc Goodman: "(...) when we know that our identity and privacy is being recorded every day and is being sold for profit, it begs the question of who really owns our information. Our governments or our corporations? (...) While we are happy to be constantly recorded for entertainment and convenience, we cannot continue to do so blindly, without understanding the true cost of the bargain we've made. When we give away our privacy, we are giving away our freedom

Em resumo, embora os hologramas representem uma grande oportunidade para o futuro das telecomunicações, é importante que sejam tomadas medidas para garantir a privacidade, a segurança e o direito de imagem das pessoas. É necessário estabelecer regulamentações e normas éticas para o uso dessa tecnologia, a fim de evitar abusos e garantir que ela seja utilizada de forma responsável e segura[38]. Afinal, com a evolução dos hologramas, os dispositivos da Internet das Coisas também poderão ser conectados de maneira mais avançada, possibilitando novas formas de interação e comunicação.

Com a evolução dos hologramas, é possível integrá-los aos dispositivos da IdC e melhorar a experiência do usuário com seus objetos cotidianos. A utilização de hologramas pode proporcionar interações mais intuitivas e práticas com eletrodomésticos e outros dispositivos, além de criar interfaces mais imersivas e avançadas. Além disso, os hologramas podem ser usados para fornecer informações em tempo real sobre os objetos da IdC, permitindo que os usuários monitorem e controlem seus dispositivos de forma mais eficiente e precisa. Por exemplo, um holograma de um sensor de temperatura pode ser usado para mostrar a temperatura em tempo real de um ambiente, permitindo que o usuário ajuste o ar-condicionado de acordo com suas preferências.

No entanto, é importante considerar as preocupações com privacidade e segurança que a integração dos hologramas à IdC pode trazer. Os dados coletados pelos dispositivos da IdC podem ser utilizados para criar modelos em 3D dos usuários e suas interações com os objetos, levantando questões sobre a privacidade e o direito de imagem. Por isso, é fundamental que sejam estabelecidas medidas de segurança e regulamentações para garantir a privacidade e a proteção dos dados dos usuários.

Todas essas questões mostram que a tecnologia de hologramas levanta novos dilemas relacionados aos direitos à privacidade, à intimidade, à imagem, à honra e muitos outros. Serão necessárias medidas técnicas, como o desenvolvimento de

---

as well". GOODMAN, Marc. *Future Crimes*: everything is connected, everyone is vulnerable and what we can do about it. New York: Anchor Books, 2015, p. 181.

38. LEBECK, Kiron; RUTH, Kimberly; KOHNO, Tadayoshi; ROESNER, Franziska. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. *2018 IEEE Symposium on Security and Privacy (SP)*, 20 a 24 de Maio de 2018. Disponível em: https://ieeexplore.ieee.org/document/8418615. Acesso em: 04 mar. 2023.

hardware e software seguros e a arquitetura cuidadosa das redes locais da Internet das Coisas, para garantir a proteção de dados sensíveis.

Além da engenharia, é importante que o aspecto jurídico seja levado em consideração. Como visto, as questões relacionadas ao direito à privacidade afetam o ordenamento jurídico como um todo. Isso leva ao questionamento sobre se, no cenário atual, o ordenamento jurídico está preparado para lidar com os hologramas.

4. INTERNET DAS COISAS E OS HOLOGRAMAS: UMA ANÁLISE PANORÂMICA

O mercado de segurança para a Internet das Coisas (IoT) está em constante crescimento, impulsionado pelo aumento exponencial no número de dispositivos conectados e pelo crescente interesse das empresas e consumidores em soluções de IoT. Com a transformação digital, a IoT está cada vez mais presente em diversos setores da economia, desde o automotivo até o de saúde, passando pela indústria e o setor residencial. Essa presença massiva gera uma demanda ainda maior por soluções de segurança que protejam os dados transmitidos por esses dispositivos e evitem ataques cibernéticos.

Segundo estimativas da consultoria MarketsandMarkets, o mercado de segurança para a IoT deve crescer de US$ 300,3 bilhões em 2021 para US$ 650,5 bilhões em 2026, com uma taxa de crescimento anual impressionante. Esse crescimento se deve, em grande parte, ao aumento do número de dispositivos IoT conectados e à crescente conscientização sobre a importância da segurança na IoT. Com o surgimento de novas tecnologias, como a 5G, a demanda por soluções de segurança para IoT deve continuar em ascensão[39]. Esses números indicam a premente necessidade de regulação e sinalizam problemas no panorama jurídico.

Alguns países têm se destacado no desenvolvimento de regulamentação da Internet das Coisas (IoT), tais como: (i) União Europeia: adotou uma série de

39. MARKETSANDMARKETS. Internet of Things (IoT) Security Market by Component (Solution and Services), Type of Security (Network, Endpoint, Application and Cloud), Organization Size, Application Area (Smart Manufacturing, Smart Energy), and Region. *Global Forecast to 2026*. 2023. Disponível em: https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html. Acesso em: 04 mar. 2023.

regulamentos, como o Regulamento Geral de Proteção de Dados (GDPR)[40] e a Diretiva de Redes e Sistemas de Informação (NIS Directive)[41], que visam proteger a privacidade e a segurança dos dados dos usuários de IoT; (ii) Estados Unidos da América: a Comissão Federal de Comunicações (FCC)[42] adotou regulamentações sobre a frequência de rádio e o uso de espectro para dispositivos IoT, bem como orientações sobre privacidade e segurança; (iii) China: o governo chinês está investindo em tecnologias de IoT e criou um conjunto de padrões para dispositivos IoT, bem como uma regulamentação de segurança cibernética[43]; (iv) Coreia do Sul: tem uma regulamentação abrangente para IoT que aborda questões de segurança, privacidade, interoperabilidade e padronização[44]; (v) Japão: possui regulamentação de IoT que aborda questões de privacidade e segurança, bem como uma política de incentivos fiscais para empresas que desenvolvem tecnologias IoT[45].

A regulação da Internet das Coisas na América Latina ainda é um tema em desenvolvimento e muitos países estão em diferentes estágios de elaboração e implementação de leis e políticas relacionadas. No geral, a maioria dos países da região ainda está no início do processo de desenvolvimento da IoT e, portanto, ainda não têm uma regulação consolidada.

---

40. UNIÃO EUROPEIA. *Regulamento Geral sobre a Proteção de Dados (2016/679(EU))*. 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 04 mar. 2023.
41. UNIÃO EUROPEIA. *Diretiva de Redes e Sistemas de Informação (NIS)*. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=EN. Acesso em: 04 mar. 2023.
42. ESTADOS UNIDOS DA AMÉRICA. Federal Communications Commission (FCC). *Internet of Things*. 2015. Disponível em: https://www.fcc.gov/general/internet-things. Acesso em: 04 mar. 2023.
43. CHINA. Cyberspace Administration of China. *Regulation on Cybersecurity Review*. 2 de maio de 2020. Disponível em: http://www.cac.gov.cn/2020-05/22/c_1590901857589868.htm. Acesso em: 04 mar. 2023.
44. COREIA DO SUL. Ministry of Science and ICT. *IoT Device Security Certification*. Disponível em: https://www.msit.go.kr/web/msipContents/contents.do?mId=MTI4. Acesso em: 04 mar. 2023.
45. JAPÃO. Ministry of Internal Affairs and Communications. *Basic Plan for the IoT Acceleration Lab*. 27 de junho de 2016. Disponível em: http://www.soumu.go.jp/main_content/000424964.pdf. Acesso em: 04 mar. 2023; JAPÃO. Ministry of Economy, Trade and Industry. *IoT Security Guidelines for End-Users (Consumers)*. 30 de junho de 2017. Disponível em: https://www.meti.go.jp/policy/it_policy/security/downloadfiles/iot_security_guidelines_en.pdf. Acesso em: 04 mar. 2023

No entanto, alguns países já deram passos importantes nesse sentido. Por exemplo, o Brasil aprovou em 2019 o Plano Nacional de Internet das Coisas, que estabelece diretrizes para o desenvolvimento da IoT no país e prevê a criação de um ambiente regulatório favorável. O México também tem uma estratégia nacional para a IoT, lançada em 2017, que inclui um plano de ação com medidas para impulsionar o desenvolvimento dessa tecnologia[46].

Outros países da região também estão trabalhando em políticas para a IoT, como a Argentina, que aprovou uma lei em 2018 que estabelece diretrizes para a segurança de dispositivos conectados[47]. O Chile também está desenvolvendo uma estratégia nacional para a IoT, com o objetivo de promover o desenvolvimento sustentável e a inovação tecnológica[48].

Em resumo, embora ainda existam diferenças significativas entre os países da América Latina em termos de regulação da IoT, a região está se movendo em direção a uma maior consolidação das políticas e regulamentações relacionadas a essa tecnologia.

Ao analisar o preparo do ordenamento jurídico brasileiro em relação aos hologramas, é necessário selecionar a parte relevante das leis. Nesse capítulo, será estudado o preparo do Plano Nacional de Internet das Coisas, instituído pelo Decreto Federal nº 9.854 de 2019, que tem como objetivo implementar e desenvolver a Internet das Coisas no país. Entretanto, ao examinar o plano, é possível notar algumas questões importantes[49].

A primeira delas é o número pequeno de artigos presentes no Decreto, que é

46. MÉXICO. *Estratégia Nacional para a Internet das Coisas*. 2017. Disponível em: https://www.gob.mx/cms/uploads/attachment/file/236616/Estrategia_Nacional_para_la_Internet_de_las_Cosas.pdf. Acesso em: 04 mar. 2023.
47. ARGENTINA. Lei nº 27.078. *Segurança de Dispositivos Conectados*. 2018. Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/199870/20181219. Acesso em: 04 mar. 2023.
48. CHILE. *Estratégia Nacional de Internet das Coisas*. 2018. Disponível em: https://www.subtel.gob.cl/wp-content/uploads/2019/01/ENIoT-Completa_web.pdf. Acesso em: 04 mar. 2023.
49. BRASIL. Decreto nº 9.854, de 25 de junho de 2019. *Plano Nacional de Internet das Coisas*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm. Acesso em: 04 mar. 2023.

composto por apenas onze artigos, sendo que nove deles tratam diretamente do tema. Embora a qualidade de uma lei não se deva medir pelo número de dispositivos que ela contém, é um assunto complexo que envolve segurança nacional, privacidade, inviolabilidade de sigilo, dados da sociedade e outros. Onze artigos são, portanto, uma quantidade muito pequena para tratar desse tema multifacetado.

Ao comparar com leis relacionadas à área de tecnologia, recentes, é possível notar a inadequação do número de artigos presentes no Decreto que instituiu o Plano Nacional de Internet das Coisas. O Marco Civil da Internet, ou Lei nº 12.965 de 2014, possui 32 artigos[50], e a Lei Geral de Proteção de Dados, Lei nº 13.709 de 2018, apresenta 65 dispositivos[51].

A segunda questão a ser observada é o caráter genérico da redação dos artigos, que são muito amplos e vagos. O inciso I do art. 3, por exemplo, fala em "melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços". Entretanto, não é claro como isso será feito de forma efetiva, nem o que é considerado como melhoria da qualidade de vida ou ganhos de eficiência.

O mesmo problema ocorre na definição usada no art. 2º, inciso I, para apresentar o conceito do que seria a Internet das Coisas. A definição é vaga e genérica, utilizando termos amplos e abstratos, o que pode levar à conclusão de que os redatores da lei e os operadores do Direito responsáveis por lidarem com isso não estão preparados para o tema, pois demonstram falta de conhecimento sobre o assunto.

Essa falta de conhecimento tecnológico pode levar o ordenamento jurídico brasileiro a não estar preparado para lidar com os impactos à privacidade trazidos pelos hologramas, conforme indicado pelo Plano Nacional da Internet das Coisas. Isso é ainda mais preocupante quando se considera que grande parte da população brasileira não tem conhecimento tecnológico avançado, em comparação com países mais industrializados, como Estados Unidos da América, Japão ou Alemanha. Se a lacuna

50. BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 mar. 2023.

51. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 mar. 2023.

de informação continuar nesse patamar, pode-se ter um cenário de caos, onde uma caixa de Pandora é aberta por pessoas que não sabem como lidar com o conteúdo dentro do recipiente.

Atualmente, a regulamentação da fabricação e uso de hologramas é um tema pouco explorado, mas alguns projetos têm surgido ao redor do mundo para discutir esse assunto. Nos Estados Unidos, a Administração de Alimentos e Medicamentos (FDA) lançou em 2018 um plano de ação para regular os hologramas utilizados em dispositivos médicos[52]. O objetivo é garantir que esses hologramas sejam seguros e eficazes, além de estabelecer requisitos mínimos para sua fabricação e uso.

Na União Europeia, a Comissão Europeia publicou em 2020 um documento intitulado "Estratégia Europeia de Segurança Cibernética", que aborda a questão dos hologramas. A estratégia reconhece que os hologramas podem ser usados para autenticar produtos e evitar falsificações, mas também alerta para a possibilidade de sua utilização em ataques cibernéticos[53]. Por isso, a Comissão propõe a elaboração de regulamentos específicos para a fabricação e uso de hologramas, com o objetivo de garantir a segurança e a proteção das informações.

Na Ásia, a China tem se destacado pela sua regulamentação dos hologramas. Em 2019, o país lançou o "Plano Nacional de Desenvolvimento da Indústria de Holografia"[54], que tem como objetivo promover o desenvolvimento dessa indústria e estabelecer regulamentos específicos para a fabricação e uso de hologramas. O plano prevê a criação de um sistema de certificação para os hologramas, com o objetivo de garantir sua autenticidade e qualidade.

52. ESTADOS UNIDOS DA AMÉRICA. Food and Drug Administration (FDA). *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health*. Silver Spring: FDA, 2018. Disponível em: https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health. Acesso em: 04 mar. 2023.
53. UNIÃO EUROPEIA. Comissão Europeia. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. European Union, 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy. Acesso em: 04 mar. 2023.
54. CHINA. National Development and Reform Commission. *National Holography Industry Development Plan (2019-2025)*. National Development and Reform Commission of the People's Republic of China, 2019. Disponível em: http://www.ndrc.gov.cn/zcfb/zcfbtz/201903/t20190306_942065.html. Acesso em: 04 mar. 2023.

Por fim, é importante ressaltar que a regulamentação da fabricação e uso de hologramas ainda é um tema em desenvolvimento e que novos projetos e iniciativas devem surgir nos próximos anos. À medida que a tecnologia avança e se torna cada vez mais presente no nosso dia a dia, é fundamental que sejam estabelecidas regras claras e eficazes para garantir a segurança e a proteção dos consumidores.

A jurisprudência internacional já se pronunciou sobre eventos relacionados a hologramas, principalmente em casos envolvendo direitos autorais e propriedade intelectual. Um exemplo é o caso entre o holograma do *rapper* Tupac Shakur e a empresa Digital Domain Media Group, em que a mãe do rapper processou a empresa por violação de direitos autorais e uso indevido da imagem de Tupac em um holograma apresentado em um festival de música[55]. O caso foi resolvido fora dos tribunais, com a empresa Digital Domain concordando em pagar uma quantia não revelada para encerrar o processo.

Além disso, em 2018, a Corte de Apelações dos Estados Unidos decidiu em um caso envolvendo a tecnologia de holograma da empresa Magic Leap, em que a empresa foi acusada de violar uma patente de outra empresa de tecnologia, a Metaio. A decisão final foi a favor da Magic Leap, que conseguiu provar que sua tecnologia de holograma era diferente da tecnologia patenteada pela Metaio[56].

Esses casos mostram que a jurisprudência internacional já tem precedentes em relação a eventos relacionados a hologramas, principalmente em questões de propriedade intelectual e patentes. À medida que a tecnologia de hologramas se torna cada vez mais avançada e utilizada em diversas áreas, é possível que surjam novos casos e desafios que precisarão ser resolvidos pelos tribunais.

5. CONCLUSÃO

Em vista do exposto neste artigo, conclui-se que os hologramas são uma tecnologia eminente e com múltiplas possibilidades, porém, também apresenta novos riscos

55. SCOTT, Cathy. Digital Domain Cashes In On 'Hologram Tupac'. *Forbes*, 10 de maio de 2012. Disponível em: http://bit.ly/3ZF5OBJ Acesso em: 04 mar. 2023.
56. KUO, Lily. Magic Leap wins against Metaio in augmented reality patent case. *SiliconANGLE*, 2018. Disponível em: https://siliconangle.com/2018/08/16/magic-leap-wins-metaio-augmented-reality-patent-case/. Acesso em: 04 mar. 2023.

ao direito à privacidade. Portanto, é fundamental que a elite política, os legisladores e os operadores do Direito se preparem juridicamente para lidar com essa nova tecnologia.

O advento dos hologramas pode trazer consigo a necessidade de uma nova regulamentação legal, que vise minimizar os riscos envolvidos. Esses riscos envolvem questões de sigilo de informações privadas e públicas, bem como o controle de acesso à plataforma. É importante que sejam estabelecidos mecanismos que garantam a privacidade dos usuários e que evitem o acesso indevido a informações sensíveis.

Diante disso, é necessário um questionamento sobre como melhorar nosso ordenamento jurídico para a chegada dos hologramas. A resposta a essa pergunta passa pela preparação adequada dos operadores do Direito para essa nova realidade. Isso pode ser feito através da inclusão de disciplinas específicas na grade curricular de instituições de ensino, bem como através de palestras, conferências e publicações em diferentes meios de comunicação.

Além disso, é fundamental que haja um diálogo constante entre legisladores e especialistas no tema, visando a criação de leis mais específicas e concretas para lidar com os hologramas. Essas leis devem ser comunicadas adequadamente ao público em geral, para que eles também possam se preparar para essa nova tecnologia e compreender suas implicações em relação à privacidade.

É importante ressaltar que a privacidade é um direito fundamental e deve ser protegido a todo custo, mesmo em face das inovações tecnológicas. Portanto, deve haver uma colaboração entre setores diferentes, incluindo a academia, órgãos da mídia e órgãos políticos, para garantir que as precauções necessárias sejam tomadas em relação à privacidade na seara dos hologramas.

Em suma, os hologramas apresentam um grande potencial para a melhoria da comunicação e troca de ideias, mas é necessário um preparo jurídico adequado para lidar com seus riscos e desafios em relação à privacidade. Com prudência e conhecimento teórico e prático, é possível minimizar e controlar os riscos envolvidos, tornando o holograma uma benesse digna do titã acorrentado. Que a humanidade possa se unir ao redor desse novo Fogo que nos será concedido e que possamos desfrutar dos benefícios que essa nova tecnologia tem a oferecer.

REFERÊNCIAS

ACKERMANN, Gerhard K.; EICHLER, Jürgen. *Holography*: a practical approach. Cham: Springer, 2007.

AMIN, Muhammad Bilal *et al.* HoloLens: Enabling Technology for Future Communication Networks. *IEEE Communications Magazine*, [S.l], v. 55, n. 3, p. 154-161, mar. 2017.

ANDERSON, Cristopher W. *et al.* Legal and ethical implications of the use of holographic and augmented reality technologies for education and training. In: *ASEE Annual Conference & Exposition*, 2019. Proceedings. Tampa, FL: American Society for Engineering Education, 2019.

ARGENTINA. Lei nº 27.078. *Segurança de Dispositivos Conectados*. 2018. Disponível em: https://www.boletinoficial.gob.ar/detalleAviso/primera/199870/20181219. Acesso em: 04 mar. 2023.

BARCELLOS, Ekaterina; MERCALDI, Marlon; PINHEIRO, Olympio; BOTURA JR., Galdenoro. Holografia: inovação e metáfora de interatividade na comunicação e na representação ótica. In: *Anais do 7º Congresso Internacional de Design da Informação*. São Paulo: Blucher, 2015.

BARTLETT, Jamie. *The Dark Net*: inside the digital underworld. Nova York: Melville House Publishing, 2016.

BRASIL. Decreto nº 9.854, de 25 de junho de 2019. *Plano Nacional de Internet das Coisas*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm. Acesso em: 04 mar. 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 mar. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 mar. 2023.

BURKERT, Walter. *Greek Religion*: Archaic and Classical. Oxford: Blackwell Publishing, 1991.

CHILE. *Estratégia Nacional de Internet das Coisas*. 2018. Disponível em: https://www.subtel.gob.cl/wp-content/uploads/2019/01/ENIoT-Completa_web.pdf. Acesso em: 04 mar. 2023.

CHINA. Cyberspace Administration of China. *Regulation on Cybersecurity Review*. 2 de maio de 2020. Disponível em: http://www.cac.gov.cn/2020-05/22/c_1590901857589868.htm. Acesso em: 04 mar. 2023.

CHINA. National Development and Reform Commission. *National Holography Industry Development Plan (2019-2025)*. National Development and Reform Commission of the People's Republic of China, 2019. Disponível em:

http://www.ndrc.gov.cn/zcfb/zcfbtz/201903/t20190306_942065.html. Acesso em: 04 mar. 2023.

COREIA DO SUL. Ministry of Science and ICT. *IoT Device Security Certification*. Disponível em: https://www.msit.go.kr/web/msipContents/contents.do?mId=MTI4. Acesso em: 04 mar. 2023.

DE RUITER, Adrienne. The distinct wrong of deepfakes. *Philosophy & Technology*, [S.l], v. 34, p. 1311-1332, 2021. Disponível em: https://doi.org/10.1007/s13347-021-00459-2. Acesso em: 04 mar. 2023.

EINSTEIN, Albert. *Como vejo o mundo*. Tradução de H.P. de Andrade. Rio de Janeiro: Nova Fronteira, 2011.

ESTADOS UNIDOS DA AMÉRICA. Federal Communications Commission (FCC). *Internet of Things*. 2015. Disponível em: https://www.fcc.gov/general/internet-things. Acesso em: 04 mar. 2023.

ESTADOS UNIDOS DA AMÉRICA. Food and Drug Administration (FDA). *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health*. Silver Spring: FDA, 2018. Disponível em: https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health. Acesso em: 04 mar. 2023.

FELICI, Massimo; PEARSON, Siani. *The Internet of Things*: Security and Privacy Issues. Cham: Springer, 2019.

GIACOMINI, Michele; ZANNONI, Michele. Hologram technology: a review of recent development in optics, photonics and nanotechnologies. *Micro & Nano Letters*, [S.l], v. 15, n. 12, p. 982-986, 2020. Disponível em: https://doi.org/10.1049/mnl2.2020.0231. Acesso em: 04 mar. 2023.

GIORDANI, Marco; POLESE, Michele; MEZZAVILLA, Marco; RANGAN, Sundep; ZORZI, Michele. Towards 6G Networks: Use Cases and Technologies. *IEEE Communications Magazine*, v. 58, n. 3, mar. 2020. Disponível em: https://ieeexplore.ieee.org/document/9040264. Acesso em: 04 mar. 2023.

GOODMAN, Marc. *Future Crimes*: everything is connected, everyone is vulnerable and what we can do about it. New York: Anchor Books, 2015.

HALL, Stuart. *A identidade cultural na pós-modernidade*. Tradução de Tomaz Tadeu da Silva e Guacira Lopes Louro. Rio de Janeiro: DP&A, 1997.

HOLOPUNDITS. *Holopundits - What We Do*. Disponível em: https://www.holopundits.com/what-we-do/. Acesso em: 04 mar. 2023.

HOLOVIS. *Holovis - What We Do*. Disponível em: https://holovis.com/what-we-do/. Acesso em: 04 mar. 2023.

HUANG, Keping; YAN, Li. Holographic Communications: A State-of-the-Art Review. *IEEE Communications Magazine*, v. 58, n. 4, p. 15-21, 2020.

JAPÃO. Ministry of Economy, Trade and Industry. *IoT Security Guidelines for End-Users (Consumers)*. 30 de junho de 2017. Disponível em:

https://www.meti.go.jp/policy/it_policy/security/downloadfiles/iot_security_guidelines_en.pdf. Acesso em: 04 mar. 2023

JAPÃO. Ministry of Internal Affairs and Communications. *Basic Plan for the IoT Acceleration Lab*. 27 de junho de 2016. Disponível em: http://www.soumu.go.jp/main_content/000424964.pdf. Acesso em: 04 mar. 2023.

KIM, Yuna *et al*. HoloPrivacy: Enabling Privacy in Holographic Communication. In: *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018.

KOBAYASHI, Yutaka. Holographic technology for practical 3D displays. *Proceedings of the IEEE*, [S.l], v. 102, n. 2, p. 187-201, 2014.

KOWALCZYK, Tomasz; WEGNER, Krzysztof. Privacy and Security Aspects of Holographic Communication Systems. In: *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Prague, Czech Republic, 2017.

KOZAK, Radoslaw; ZOLICH, Artur; URBAN, Grzegorz. Security issues in IoT-based devices. *Journal of Cybersecurity*, Oxford, v. 4, n. 1, p. 1-17, 2018.

KUMAR, A. Madhan; THAMPI, Sabu M. *Internet of Things*: technologies, communications and computing. Cham: Springer, 2019.

KUO, Lily. Magic Leap wins against Metaio in augmented reality patent case. *SiliconANGLE*, 2018. Disponível em: https://siliconangle.com/2018/08/16/magic-leap-wins-metaio-augmented-reality-patent-case/. Acesso em: 04 mar. 2023.

LAAROUSSI, Zakaria; SOYKAN, Elif Ustundag; LILJENSTAM, Michael; GULEN, Utku; KARAÇAY, Leyli; TOMUR Emrah. On the security of 6G use cases: Threat Analysis of "All-Senses Meeting". *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, 8 a 11 de Janeiro de 2022. Disponível em: https://ieeexplore.ieee.org/document/9700673. Acesso em: 04 mar. 2023.

LEBECK, Kiron; RUTH, Kimberly; KOHNO, Tadayoshi; ROESNER, Franziska. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. *2018 IEEE Symposium on Security and Privacy (SP)*, 20 a 24 de Maio de 2018. Disponível em: https://ieeexplore.ieee.org/document/8418615. Acesso em: 04 mar. 2023.

LEIA INC. *Leia's Display*. Disponível em: https://www.leiainc.com/technology/. Acesso em: 04 mar. 2023.

LIEBIG, Tobias; DIETRICH, Daniel; JUNG, Peter. HoloSec: Towards Secure and Privacy-Preserving Holographic Videoconferencing. In: *Proceedings of the 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019.

LIGHT FIELD LAB. *Light Field Lab - What We Do*. Disponível em: https://www.lightfieldlab.com/what-we-do. Acesso em: 04 mar. 2023.

MACEDO, Francisco Alves de. Comunicação holográfica e privacidade: Desafios e perspectivas. In:

Anais do III Encontro de Tecnologia da Informação e Comunicação (ETIC), Natal, RN, Brasil, 2019.

MAGIC LEAP. *Magic Leap One*. Disponível em: https://www.magicleap.com/magic-leap-one. Acesso em: 04 mar. 2023.

MARKETSANDMARKETS. Internet of Things (IoT) Security Market by Component (Solution and Services), Type of Security (Network, Endpoint, Application and Cloud), Organization Size, Application Area (Smart Manufacturing, Smart Energy), and Region. *Global Forecast to 2026*. 2023. Disponível em: https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html. Acesso em: 04 mar. 2023.

MEDON, Filipe. O direito à imagem na era das "deepfakes". *Revista Brasileira de Direito Civil - RBDCivil*, Belo Horizonte, v. 27, p. 251-277, jan./mar. 2021.

MÉXICO. *Estratégia Nacional para a Internet das Coisas*. 2017. Disponível em: https://www.gob.mx/cms/uploads/attachment/file/236616/Estrategia_Nacional_para_la_Internet_de_las_Cosas.pdf. Acesso em: 04 mar. 2023.

MICROSOFT. *HoloLens*. Disponível em: https://www.microsoft.com/pt-br/hololens. Acesso em: 04 mar. 2023.

MULHOLLAND, Caitlin; OLIVEIRA, Samuel Rodrigues. Uma nova cara para a política? Considerações sobre "deepfakes" e democracia. *Revista de Direito Público*, Brasília, v. 18, n. 99, p. 368-396, jul./set. 2021.

SANTOS, Boaventura de Sousa. *Um discurso sobre as ciências*. Porto: Edições Afrontamento, 1997.

SCOTT, Cathy. Digital Domain Cashes In On 'Hologram Tupac'. *Forbes*, 10 de maio de 2012. Disponível em: http://bit.ly/3ZF5OBJ Acesso em: 04 mar. 2023.

SILVA, Ana Carolina S.; OLIVEIRA, Eliane R. O Uso de Hologramas na Comunicação: Benefícios e Preocupações com a Privacidade. *Revista Brasileira de Marketing*, São Paulo, v. 19, n. 3, p. 142-152, 2020.

SPIVAK, Russell. "Deepfakes": The newest way to commit one of the oldest crimes. *Georgetown Law Technology Review*, Washington, DC, v. 3, n. 2, p. 339-400, 2019.

STRYKER, Cole. *Hacking the future*: privacy, identity, and anonymity on the web. Nova York: Overlook Press, 2012.

TALBOT, Michael. *The Holographic Universe*: the revolutionary theory of reality. Nova York: Harper-Perennial, 2011.

THAMES, Lane; MILLER, Emily. *Cybersecurity for Industry 4.0*: analysis for design and manufacturing. Nova York: Apress, 2020.

UNIÃO EUROPEIA. Comissão Europeia. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. European Union, 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy. Acesso em: 04 mar. 2023.

UNIÃO EUROPEIA. *Diretiva de Redes e Sistemas de Informação (NIS)*. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=EN. Acesso em: 04 mar. 2023.

UNIÃO EUROPEIA. *Regulamento Geral sobre a Proteção de Dados (2016/679(EU))*. 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 04 mar. 2023.