INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 04 · n. 01 · janeiro/abril 2023 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.4.n.1

04

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

IJDL – INTERNATIONAL JOURNAL OF DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM
Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Rua Paulo Ribeiro Bastos, 211 – Jardim Atlântico – CEP 31710-430
Belo Horizonte/MG – Brasil – Tel.: (31) 99412.0131
www.editoraforum.com.br / E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil / Distribuída em todo o Território Nacional

IN61 International Journal of Digital Law – IJDL. – ano 1, n. 1 (abr. 2020) –.– Belo Horizonte: Fórum, 2020-.

Quadrimestral; Publicação eletrônica
ISSN: 2675-7087

1. Direito. 2. Direito Digital. 3. Teoria do Direito. I. Fórum.

CDD: 340.0285
CDU: 34.004

Coordenação editorial: Leonardo Eustáquio Siqueira Araújo
Aline Sobreira
Capa: Igor Jamur
Projeto gráfico: Walter Santos

Sumário
Contents

DOI: 10.47975/digital.law.vol.4.n.1.valle

Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT[I]

The challenges regarding the preservation of privacy and data protection in the face of the IoT equipment

Vivian Lima López Valle[*]
Pontifícia Universidade Católica do Paraná (Curitiba, Paraná, Brasil)
vivianclvalle@gmail.com
https://orcid.org/0000-0002-5793-2912

Bruna Gavron Barbosa[**]
Pontifícia Universidade Católica do Paraná (Curitiba, Paraná, Brasil)
brunagavron@hotmail.com
https://orcid.org/0009-0008-8723-9052

Recebido/Received: 03.03.2023/ March 3rd, 2023
Aprovado/Approved: 09.06.2023/ June 9th, 2023

Resumo: A Internet das Coisas poderá alterar significativamente o modo como as pessoas vivem. Entretanto, com a crescente utilização desses dispositivos, que já se encontram ou que estarão em breve no mercado, é necessária uma atenção aos riscos que eles podem trazer à privacidade como

[I] Como citar esse artigo/How to cite this article: VALLE, Vivian Lima López; BARBOSA, Bruna Gavron. Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT. *International Journal of Digital Law, Belo Horizonte*, v. 4, n. 1, p. 35-61, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.valle.

* Professora titular de Direito Administrativo da Pontifícia Universidade Católica do Paraná (Curitiba, Paraná, Brasil). Doutora e mestre em Direito do Estado pela Universidade Federal do Paraná. Especialista em Contratação Pública pela Universidade de Coimbra. Coordenadora do Curso de Direito da Pontifícia Universidade Católica do Paraná. Coordenadora do Curso de Especialização em Licitações e Contratos da Pontifícia Universidade Católica do Paraná. Diretora acadêmica do Instituto Paranaense de Direito Administrativo. Membro da Comissão de Gestão Pública da Ordem dos Advogados do Brasil, Seção Paraná. Advogada especializada em Direito Público. *E-mail*: vivianclvalle@gmail.com.

** Bacharela em Direito pela Pontifícia Universidade Católica do Paraná (Curitiba, Paraná, Brasil). Advogada. *E-mail*: brunagavron@hotmail.com.

direito fundamental dos usuários. Assim, o objetivo do presente artigo é demonstrar os desafios para preservação do direito à privacidade como princípio constitucional, frente à crescente conectividade dos dispositivos presentes no cotidiano dos indivíduos, visando à aplicação do princípio da privacidade, no âmbito da Internet das Coisas (IoT), e com base na Constituição Federal e na Lei Geral de Proteção de Dados.

Palavras-chave: LGPD. IoT. Privacidade. Tecnologia. Dados. iRobot.

The challenges regarding the preservation of privacy and data protection in the face of the IoT equipment

Abstract: The Internet of Things could significantly change the way people live. However, with the use of these devices that are already on the market, it is necessary to pay attention to the risks that can bring to privacy as the fundamental right of users. Thus, the objective of the article is to demonstrate the challenges for the preservation of the right to privacy as a constitutional principle, the growing connectivity of devices in the daily life of the base, applying the application of the principle of privacy in the scope of the Internet of Things (IoT), with basis on the Federal Constitution and on the General Data Protection Law.

Keywords: GDPR. IoT. Privacy. Technology. Data. iRobot.

1 Introdução

A proposta da presente pesquisa consiste em abordar os desafios na preservação da privacidade como princípio constitucional frente ao avanço da tecnologia, visando demonstrar a fragilidade dos equipamentos cada vez mais conectados e dependentes da internet, utilizando-se dos parâmetros resguardados pela Lei nº13.709/2018 (Lei Geral de Proteção de Dados).

O ponto inicial é o impacto causado pelo avanço da tecnologia, que expandiu celeremente a conectividade dos dispositivos eletrônicos e objetos diversos, causando uma enorme concessão de dados pelos seus usuários, uma vez que, para seu funcionamento, há uma vasta coleta e envio de dados que estes adquirem de seus ambientes. É certo que em uma sociedade de comunicação digital, desde as redes e mídias sociais à Internet das Coisas, também conhecida por IoT (Internet of Things, em inglês), a violação de sua privacidade tem colocado em risco o sistema constitucional com seus mecanismos de proteção dos direitos.

Em razão disso, tal estudo conceituará o direito à privacidade como direito fundamental resguardado pela Constituição Federal de 1988. Posteriormente, adentrará na aplicação deste no âmbito da Internet das Coisas (IoT), a qual descreve uma rede de objetos físicos incorporados a sensores, *software* e outras tecnologias, com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela

internet. Esses dispositivos variam de objetos domésticos comuns a ferramentas industriais sofisticadas.

Partindo dessa premissa, o estudo apontará os desafios para a aplicação do direito à privacidade na esfera da IoT frente aos dispositivos legais resguardados pela Lei Geral de Proteção de Dados, uma vez que ela permite o compartilhamento e coleta de dados com o mínimo de intervenção humana, de modo que tais sistemas podem digitais gravar, monitorar e ajustar cada interação entre itens conectados.

2 A relevância da *internet* na sociedade de informação

Ao longo do tempo, a sociedade passou por diversas formas de organização social. Cada mudança teve por fator determinante a estruturação de um elemento central que, ao seu desenvolvimento, estabeleceu o respectivo marco histórico.[1]

Na sociedade agrícola, o produto agrícola era o fator determinante para a economia por meio da prática do escambo (que de modo geral significa troca ou permuta), sendo a fonte de riqueza aquilo que provinha da terra. Na sociedade industrial, a fonte de riqueza sobreveio da criação das máquinas a vapor e da eletricidade, que modificou a produção nas fábricas.[2]

Em um terceiro momento, na sociedade dita sociedade pós-industrial, a prestação de serviço passou a impulsionar a economia, ou seja, mais importante era não mais o que se produzia, mas como poderia se ofertar os serviços.[3]

Já na sociedade atual, a forma de organização tem como seu elemento central a informação, sendo essa a impulsionadora da economia. Esse elemento se consolidou devido à acelerada evolução tecnológica, da qual decorrem vários mecanismos capazes de processar e transmitir informações em quantidade e velocidade inimagináveis. A relação social foi afetada por um amontoado de informações; não havia mais obstáculos físicos, como a distância, que pudessem interferir, o que também gerou uma nova compreensão de tempo-espaço.[4]

Sobre tal perspectiva, é possível dizer que a informação é o novo elemento estruturante responsável pela organização da sociedade, assim como foram a terra, as máquinas a vapor e a eletricidade e os serviços, formando a chamada sociedade da informação. E, ainda que essa nova forma de organização não se resuma ao ambiente virtual, as ferramentas que contribuem de forma mais abundante neste processo são a computação e a *internet*.

1 SILVA, 2009, p. 43.
2 BIONI, 2021, p 3.
3 BIONI, 2021, p. 3.
4 BIONI, 2021, p. 4.

Outro fator determinante na sociedade da informação é a alteração da plataforma na qual estas são sobrepostas. Antes, as informações eram descritas e armazenadas em papéis por meio de livros ou ficheiros. Após a descoberta dos *bits*, um sistema binário (1 e 0) que empregou uma linguagem compreensível aos computadores, passou-se a processar e armazenar informações, condensando-as em unidades menores, bem como possibilitou-se o uso de comandos pré-determinados, por exemplo, a utilização de palavras-chave com intuito de buscar informações. Com essa desmaterialização, logo todos os tipos de informações (áudio, vídeo, imagens...) também puderam ser digitalizadas, o que gerou um acúmulo de informações e novas plataformas, como *compact disk* (CD), *pendrive*, computadores pessoais, entre outros.[5]

Manuel Castells destacou, nos anos 1990, que a *internet* seria o canal de interconexão global mais importante, de modo que praticamente tudo estaria conectado a sistemas acessíveis a indivíduos e instituições, bem como afirmou que a caracterização da atual revolução tecnológica é a aplicação de novos conhecimentos e informações que geram dispositivos de processamento e comunicação da informação, de forma a se tornar um ciclo cumulativo de inovação – introdução de uma nova tecnologia – e seu uso.[6]

Com o avanço da tecnologia, o século 19 rege-se pelas múltiplas inovações das formas de comunicação na *web*, caracterizando-se pelo acesso instantâneo, pela praticidade dos aplicativos *mobile*, pela celeridade na transmissão de mensagens e, principalmente, pela enorme quantidade de dados pessoais e informações armazenadas.[7]

Essa realidade traz preocupação, uma vez que expandiu celeremente a conectividade dos dispositivos eletrônicos e objetos diversos, causando uma enorme concessão de dados pelos seus usuários, considerando-se que, para seu funcionamento, há uma vasta coleta e envio de dados que estes adquirem de seus ambientes.

É certo que, em uma sociedade de comunicação digital, desde as redes e mídias sociais à Internet das Coisas, a violação de sua privacidade tem colocado em risco o sistema constitucional com seus mecanismos de proteção dos direitos, uma vez que os usuários ficaram mais vulneráveis à violação e à quebra de sigilo de seus dados eletrônicos ou digitais. Essa vulnerabilidade cresceu junta à inovação tecnológica, sobretudo quanto à privacidade e à intimidade, que possibilitou a quebra da confidencialidade dos meios de comunicação e dados, pois, enquanto há uma grande circulação de informações pela rede, que ocasiona aumento de invasões

5 BIONI, 2021, p. 6.
6 CASTELLS, 1999, p. 69.
7 ÁVILA; WOLOSZYN, 2017.

de *e-mails* e correspondências, indesejáveis telefonemas a contatos pessoais do usuário da tecnologia, há também aplicativos capazes de assimilar quais as rotinas, as preferências comerciais e trajetos do cotidiano dos usuários.[8]

E, mesmo estando assegurado o sigilo dos dados, correspondências e comunicações por meio do sistema de proteção e defesa dos direitos humanos, sendo convencionais ou extraconvencionais, bem como tenha sido abarcado pelo texto constitucional, afirma Bobbio que a maior provocação atual é saber, com exatidão, de que forma garanti-los em meio ao sistema global digital identificado pela inexistência de limites materiais.[9]

3 Os direitos fundamentais à privacidade e à intimidade na Constituição de 1988

Os direitos à privacidade e à intimidade são duas grandes heranças dos ideais do liberalismo dos séculos 17 e 18, ambos relacionados às liberdades individuais e, por isso, resguardados no âmbito constitucional de diversos países e na maioria dos documentos que versam sobre a proteção aos direitos humanos.

No início, o direito à vida privada adquiriu seus contornos por meio da defesa da propriedade, em que o domicílio era o elemento principal compreendido como o espaço onde o indivíduo estaria protegido de terceiros e do Estado. Entretanto, com o avanço das tecnologias, o sujeito ficou mais propício a ser exposto de modo inabitual, o que tornou necessário uma compreensão mais robusta do significado do direito à vida privada. Assim, a privacidade deixou de ser compreendida apenas na esfera da propriedade, passando a ser considerada também um direito à personalidade.

Os direitos de personalidade então previstos na Constituição Federal de 1988 em seu art. 5º, em especial nos incisos X, XI e XII, os quais respectivamente tratam da proteção ao direito à vida privada, à intimidade, à inviolabilidade do domicílio, ao sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas.

A Declaração Universal dos Direitos do Homem, por meio de seu art. 12, prevê que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

Na mesma linha, estabelece a Convenção Europeia para Proteção dos Direitos Humanos e das Liberdades Fundamentais,[10] de 1950, por meio de seu art. 8º,

8 ÁVILA; WOLOSZYN, 2017, p. 168.
9 BOBBIO, 2004, p. 25 citado por ÁVILA; WOLOSZYN, 2017, p. 170.
10 COUNCIL OF EUROPE, 1950.

a Carta de Direitos Fundamentais da União Europeia,[11] em seu art. 8º, o Pacto Internacional de Direitos Civis e Políticos,[12] a proteção da privacidade, em seu artigo 17, e a Convenção Americana de Direitos Humanos, assinada pelos países membros da Organização dos Estados Americanos,[13] em 1969, em São José da Costa Rica, por meio do art. 11.

Verifica-se que os direitos à privacidade e à intimidade restam protegidos por variados regulamentos, tanto regionais quanto internacionais, de modo que é de competência de cada Estado-membro a discriminação destes em seu ordenamento jurídico e a definição da forma como será efetivada tal proteção. Entretanto, considerando a dicotomia trazida pela Constituição Federal de 1988 ao preceituar a privacidade e a intimidade, se faz necessária uma abordagem mais minuciosa de tais termos.

O direito estadunidense, o qual dispõe sobre o *right to privacy*, não distingue a privacidade da intimidade, ou direito ao segredo do direito à reserva da doutrina italiana. Trata apenas de forma genérica o direito à privacidade, o qual não deixa de ser delimitado e compreendido devidamente na doutrina norte-americana, sendo uma preocupação jurisprudencial, a qual pode ser demonstrada por meio da Quarta Emenda à Constituição dos Estados Unidos. Esta proíbe a busca e apreensão sem causa razoável e mandado judicial amparado em causa provável, e sua origem se deve a um artigo escrito por dois advogados que problematizaram a crescente e potencial invasão do governo e da mídia na vida das pessoas.[14] Em princípio, o entendimento americano sobre a privacidade desdobra-se da propriedade, limitando ao Estado o poder de invadi-la, controlá-la ou ainda de dispô-la.

A doutrina brasileira se aproxima, em parte, dessa concepção do direito estadunidense, sem distinguir, de forma clara, a privacidade da intimidade, de forma que, quando realizada tal distinção, irrelevante materialmente, tornando-se mera questão de aprofundamento material. Essa mesma linha é seguida pelos doutrinadores José Afonso da Silva,[15] Gonet Branco[16] e Luiz Avolio.[17]

Tércio Sampaio Ferraz Jr. destaca que a privacidade se rege pelo princípio da exclusividade, o qual se baseia em três atributos: a solidão ou o estar só, o segredo ou o direito de exigir o sigilo e a autonomia, ou o direito de dispor sobre si mesmo, como sendo o centro das informações. A intimidade, por sua vez, garante sobretudo o estar só, trata-se de um aprofundamento da definição de privacidade;

11 EUROPEAN UNION, 2000.
12 BRASIL, 1992a.
13 BRASIL, 1992b.
14 GARCIA, 2018, p. 6.
15 SILVA, 1989. p. 183.
16 GONET BRANCO, 2009, p. 420.
17 AVOLIO, 2012, p. 24.

ou seja, com base no âmbito da privacidade, a intimidade é o mais exclusivo dos direitos e está contido no princípio da privacidade.[18]

Ao passo que Ferraz Júnior, em sua doutrina, trata do direito à privacidade com base no direito estadunidense, Paulo José da Costa Junior[19] popularizou no Brasil a teoria das esferas do direito alemão. Essa descreve a privacidade como sendo dividida em camadas, em que a primeira camada e a mais ampla representa a esfera privada, e nela estão contidos os comportamentos e acontecimentos que o indivíduo não quer que se tornem de domínio público; já na segunda, contida no interior da primeira, está a intimidade, uma esfera confidencial da qual fazem parte indivíduos em que a pessoa deposita certa confiança e com quem mantém uma intimidade; por fim, a terceira e última camada, localizada no centro, é a esfera do segredo.

Por meio dessa teoria, é possível distinguir intimidade da vida privada, bem como diferenciá-las do segredo. Isso se justifica pois a vida privada, como esfera de maior amplitude, é o direito de impedir que fatos da vida particular cheguem ao conhecimento do público. Já a intimidade, em sentido lato, remete ao direito de excluir do saber de outros informações sensíveis do indivíduo, como dados sobre vida sexual, política e religiosa, geralmente compartilhados apenas com pessoas mais íntimas e de forma reservada. Quanto à última esfera, a do segredo, ou intimidade em sentido estrito, ela compreende informações sobre o sentimento, sonhos e emoções do indivíduo, as quais geralmente não são divulgadas a terceiros e podem ser compartilhadas com amigos mais íntimos.[20]

Apesar de as correntes doutrinárias não realizarem clara distinção entre a vida privada e a intimidade, na Constituição Federal de 1988, é expressamente prevista tal dicotomia. Devido a isso, importante é buscar compreendê-la, porém sem desconsiderar que ainda há uma área cinzenta entre os princípios da vida privada e da intimidade, em virtude da sua proximidade.

Essa distinção pode ser mais bem compreendida com o suporte literário de George Orwell, por meio da distopia *1984*, criada pelo autor em 1949, na qual não há privacidade. O protagonista Winston consegue sair da vigilância do chamado "Grande Irmão" apenas em momentos de fuga, ou quando se aproveita de falhas dos sistemas de vigilância. Isso demonstra que a privacidade pode ser facilmente mitigada pelo poder estatal; basta que haja vigilância absoluta em todos os lugares, o que impede que um indivíduo fique só ou sem que alguém o observe por um instante.

[18] FERRAZ JÚNIOR, 1993, p. 439.
[19] GARCIA, 2018, p. 9.
[20] VIEIRA, 2007, p. 30.

Apesar de essa mitigação da privacidade afrontar necessariamente a intimidade das pessoas, uma vez que impede o seu livre desenvolvimento, a violação da intimidade não está ligada apenas à privação de determinado espaço sem que haja interferência de terceiros, ou ao sigilo de aparelhos pessoais, mas também ao pensamento próprio, à crítica, à noção do indivíduo sobre si e sobre o mundo, suas emoções, sentimentos, personalidade, relacionamentos íntimos, enfim, sua dignidade.

Nesse sentido, a intimidade adquire uma amplitude semântica que vai além do direito de estar só ou do direito à propriedade, como dito anteriormente. Resulta sua violação em exposição, que traz consigo a vergonha, impotência e medo. A própria possibilidade de virem a público os pensamentos, interesses, gostos e sexualidade do indivíduo sem o seu devido consentimento atinge o livre desenvolvimento de sua personalidade e de seu modo de ser na sociedade.

De forma resumida, a privacidade está ligada historicamente à proteção da propriedade e do direito de não ser incomodado por meio de seus bens, enquanto a intimidade se relaciona à proteção do livre desenvolvimento e da personalidade. A diferenciação proposta excede a sintonia entre os princípios; entretanto, considera-se que essa distinção conceitual está mais evidente em sua definição constitucional, além de conter mais potencial sob um viés político e crítico quanto à livre consciência e aos direitos civis, o que supera a origem patrimonialista.

4 O tratamento de dados por meio da Lei Geral de Proteção de Dados como forma de preservar o direito à privacidade

Tais princípios ainda podem ser compreendidos por meio de diferentes dimensões, as quais são citadas na obra de Bart Willem Schermer: o corpo, a mente, o domicílio, o comportamento íntimo, as comunicações, a vida familiar e os dados pessoais. Contudo, considerando o objeto do presente artigo, limitar-nos-emos à abordagem dos dados pessoais.[21]

Os dados pessoais são, segundo a Lei Geral de Proteção de Dados (LGPD), toda informação relacionada à pessoa natural identificada ou identificável (art. 5º, inciso I), ou seja, todas as informações codificadas de uma determinada pessoa que, ao serem tratadas, gera um informação pessoal,[22] o que abarca endereço, Código de Endereçamento Postal (CEP), número de telefone, profissão, data de nascimento, números indicadores da documentação em geral, nome de familiares, cidade natal, número do cartão de crédito, dados bancários, endereço eletrônico,

[21] SCHERMER, 2007, p. 76.
[22] ZANON, 2018, p. 21.

salário, mensagens de texto, fotos e vídeos, endereço de Internet Protocol (IP), entre outros.

Sem dúvida, a questão sobre o tratamento de dados pessoais eleva-se em importância devido ao avanço das novas tecnologias de comunicação. Por meio da Emenda Constitucional nº115, foi incluído, na Constituição Federal de 1988, o inciso LXXIX ao art. 5º, o qual prevê que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais", podendo ainda do esvaziamento dos próprios princípios da privacidade e da intimidade verificar que estes também protegem os dados pessoais, com a finalidade de não permitir condutas invasivas, ou seja, não permitir o acesso total aos dados pessoais pelo Estado ou por terceiros, de modo a ignorar o sentido principiológico dos dispositivos.

Até mesmo na administração pública foi introduzida uma nova perspectiva sobre o potencial gerencial, econômico e de direção das atividades públicas, decorrentes do movimento global em torno da disseminação de ferramentas de tecnologia da informação (TICs) e dos instrumentos digitais de preservação e armazenamento de dados, que possuem cada vez mais capacidade. Tal concepção levou à observação de que os dados podem se transformar em informações úteis, não sendo apenas dados isolados ou "crus" (*raw data*), trazendo à administração pública o dever de adotar medidas de proteção e segurança aos indivíduos, enquanto titulares dos dados e de seus próprios agentes, responsáveis pelo tratamento das informações.[23]

A chamada Quarta Revolução Industrial permitiu a fusão dos ambientes físico, digital e biológico, possibilitando relações jurídicas e interações inimagináveis no século 20. Tal revolução exige uma regulação eficiente capaz de, ao mesmo tempo, afastar as vicissitudes causadas pelo uso indevido, mal-intencionado, discriminatório, direcionado e estandardizado dos algoritmos e não impedir as inovações disruptivas e seu potencial transformador.[24]

Atualmente, praticamente todos os dados de uma pessoa estão, de alguma forma, registrados. Exemplo, os celulares, que guardam diversas informações sobre seus usuários, o Google, o Facebook, os bancos, os registros das conversas via WhatsApp, capazes de traçar perfil detalhado da vida e dos relacionamentos pessoais da pessoa, o conteúdo armazenado em computadores pessoais etc. Com base nisso, não resta dúvida de que o acesso a essas informações é capaz de criar uma narrativa vasta e arriscada acerca do indivíduo.

Egon Bockmann Moreira indica a necessidade de se constituir direitos fundamentais para humanos digitais, citando a existência de uma minuta da Carta dos Direitos Digitais da União Europeia que expande a percepção de direitos

[23] CRISTÓVAM; HAHN, 2020, p. 7.
[24] VALLE; GALLO, 2020, p. 78.

fundamentais para o mundo digital. O autor discorre sobre a *persona* digital em uma dimensão existencial ligada à dimensão de dados, informações digitalizadas e perfis que o indivíduo analógico assume no ambiente virtual, bem como sobre a interação da Inteligência Artificial (IA) algorítmica com ela. As perguntas pertinentes sobre tal assunto são: essa nova configuração do humano digital necessita de proteção distinta e de direitos fundamentais? a *persona* digital faz jus a proteção autônoma na condição de direito fundamental como um ser digitalizado? o posicionamento de Moreira inclina-se ao fato de a *persona* digital possuir autonomia diferenciada, e é merecedor de proteção de métricas que desconhece.[25]

As expressões "dados" e "informações" são comumente usadas como sinônimas, porém, são distintas. Dados refere-se a um estado primitivo da informação; são, segundo Bruno Bioni,[26] fatos brutos que se tornam algo inteligível quando processados e organizados, do qual pode se extrair uma informação. O inciso IV do art. 5º da LGPD conceitua banco de dados como sendo um "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico", o que envolve, em sua operação, a entrada (*input*) e a manipulação de dados e a saída (*output*) de uma informação, bem como seu gerenciamento, do qual se extrai conhecimento. Quanto à expressão "informação", ela é definida como sendo um dado ou conjunto de dados, processados ou não em um suporte apto a gerar conhecimento; pode ser uma imagem, som, documento eletrônico ou físico, ou ainda um dado isolado.[27]

Com base em tais definições, verifica-se que o banco de dados não é reduzido a um repositório de informações, mas trata-se de uma ferramenta que permite a criação de uma interface que possibilita a manipulação, análise e o descobrimento de informações para tomada de decisões. Isso possibilita a identificação e determinação do perfil do potencial consumidor, bem como seus hábitos e demais informações essenciais à tomada de decisão de forma tática e estratégica. É a chamada mineração de dados ou *data mining*, em que apenas alguns dados são valiosos, o que torna necessária a realização de uma seleção destes, uma vez que os dados considerados úteis não são mais identificados como dados, mas sim como informação por conter aspectos úteis e valor agregado, de modo que a mineração busca descobrir padrões, segmentar informações ou buscar correlações entre dados existentes.

Ainda, a LGPD traz conceitos distintos para "dados pessoais", "dados pessoais sensíveis" e "dados anonimizados". Em seu art. 5º, incisos I, II e III, classifica-os da seguinte forma:

[25] MOREIRA, 2019.
[26] BIONI, 2019, p. 35.
[27] VIEIRA, 2007, p. 157.

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Com tal distinção, nota-se que os dados pessoais sensíveis são aqueles que necessitam de maior proteção e sigilo, podendo sua coleta e utilização ocorrerem com ou sem consentimento explícito do titular, se abrangido em uma das hipóteses descritas no inciso II do art. 11 da Lei nº 13.709/2018.

A LGPD é aplicada para todas as operações de manipulação de dados feitas por pessoa natural ou física, independentemente do meio, do país de sua sede ou país onde estejam situados os dados, desde que essa operação de tratamento de dados seja realizada em território nacional com objetivo de ofertar ou fornecer serviços ou bens ou o tratamento de dados individuais localizados em território nacional. Exclui-se de tal aplicação o tratamento de dados pessoais com finalidade meramente particular ou não econômico, bem como para questões de defesa nacional, segurança pública, atividades de investigação e repressão de infrações penais, fins jornalísticos, artísticos e acadêmicos (arts. 3 e 4 da lei).

Entre os princípios norteadores de tal lei, os quais estão dispostos no art. 6º, estão os princípios da necessidade (inciso III), o qual limita o tratamento ao mínimo necessário para determinada finalidade, sem que haja excesso; livre acesso (inciso IV), que garante aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento; transparência (inciso VI), que garante aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento; segurança (inciso VII), que visa À 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; prevenção (inciso VIII), que prevê a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; não discriminação (inciso IX), que impossibilita a realização do tratamento para fins discriminatórios ilícitos ou abusivos; responsabilização e prestação de contas (inciso X), que exigem a demonstração pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como a eficácia dessas medidas. Esses princípios garantem o respeito aos direitos dos titulares, bem como geram

diretrizes a serem seguidas pelos agentes de tratamento, como o consentimento do titular e o legítimo interesse.

O tratamento dos dados é toda operação que coleta, utiliza, reproduz, transmite, distribui, processa, armazena, elimina e transfere dados, conforme demonstra o Quadro 1:

Quadro 1 - Tratamento de dados

DADOS PESSOAIS	
FASE DO CICLO DE TRATAMENTO	OPERAÇÕES DE TRATAMENTO - LGPD, ART. 5º, X
Coleta	Coleta, produção, recepção.
Retenção	Arquivamento e armazenamento.
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação.
Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão.
Eliminação	Eliminação.

Fonte: Comitê Central de Governança de Dados. Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD).

Para tal tratamento, a lei prevê a figura dos agentes de tratamento, os quais são o controlador, o operador e o encarregado pelo tratamento de dados. O controlador é o responsável pelas decisões referente ao tratamento dos dados coletados. O operador é quem realiza o tratamento dos dados pessoais em nome do controlador. Para atuação de ambos os agentes, a LGPD estabelece atribuições e limites, bem como os requisitos ao tratamento dos dados, conforme dispõem os arts. 7º e 11º da lei. Já o encarregado é a pessoa indicada pelo controlador e operador para operar como meio de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Tudo isso é necessário para segurança e sigilo dos dados, de maneira que a segurança da informação não é uma preocupação apenas das empresas ou do próprio Estado que coletam e processam os dados, mas também dos titulares, que estão, hoje, mais atentos, considerando os possíveis impactos de seus dados em posse de outros. A Lei nº 13.709/2018 evidenciou a responsabilidade dos agentes de tratamento e previu que estes devem adotar medidas de segurança para garantir que os dados pessoais não sejam obtidos por acessos não autorizados ou por situações acidentais ou ilícitas que visem a alteração, perda, destruição, comunicação ou outra forma de tratamento inapropriado ou ilícito. Assim, deve

ser mantida a garantia da segurança da informação até mesmo posteriormente ao tratamento realizado.

Ocorrendo incidentes de segurança que possibilitem risco ou dano significativo aos titulares, é dever do operador comunicar de maneira imediata a ANPD, descrevendo os fatos ocorridos, as informações sobre os indivíduos (titulares) afetados, os riscos ligados ao incidente e as medidas que serão tomadas a fim de reverter os efeitos do prejuízo. De forma breve, destaca-se que a ANPD é um órgão do governo inerente à presidência da República, ao qual compete fiscalizar e executar o que prevê a LGPD, regulamentar e fiscalizar as operações de tratamento dos dados, bem como aplicar as penalidades ao descumprimento da lei.

Quanto ao modelo regulatório, uma das principais características da LGPD, a qual foi herdada da RGPD (Regulamento Geral de Proteção de Dados), é a adoção do *ex-ante*, o qual impõe que, para o tratamento de dados pessoais, antes mesmo de ser realizada a coleta ou outra ação que envolva o primeiro, deve ser o agente de tratamento capaz de justificar tais atos, com base em uma das hipóteses de tratamento previstas no art. 7º da LGPD. Tal modelo *ex-ante* parte, ainda, da premissa de que todo dado pessoal ou toda informação ligada à pessoa natural identificada ou identificável é relevante sob aspecto jurídico, o que se deve ao aumento do processamento ubíquo e automatizado dos dados, fato que traz a necessária regulamentação das diversas formas de tratamento de dados pessoais.[28]

Assim, verifica-se que a LGPD possui como principal objetivo proteger os direitos fundamentais de liberdade e privacidade dos indivíduos, concentrando regras sobre o uso adequado de dados pessoais, aplicado a todos os setores, gerando um cenário com mais segurança jurídica, padronização de regulamento e ações que visem garantir a proteção no tratamento dos dados coletados, implementando um ambiente de desenvolvimento tecnológico, a partir de normas flexíveis e adequadas ao cuidado de negócios que se baseiam no uso de dados pessoais. Por meio dessa lei, o Brasil se torna ainda apto a gerenciar dados advindos de outros países que exigem níveis de segurança de dados. A redação da LGDP contém 65 artigos que abrangem diversas situações que resguardam os direitos dos titulares dos dados, bem como normas que devem ser observadas em operações que visem ao tratamento de dados pessoais pelos controladores e operadores.

[28] ZANETTI DE OLIVEIRA; FREITAS, 2022, p. 95.

5 A proteção da privacidade nos dispositivos IoT com base na Lei Geral de Proteção de Dados

A segurança de dados e da privacidade do usuário é um dos temas mais importantes em se tratando de uma rede de dispositivos. Desse modo, se faz necessária a adoção de medidas de segurança e de gerência de dados que possibilitem mitigar ataques e preservar a integridade das informações, uma vez que, dependendo do caso concreto, pode haver dados sensíveis armazenados ou em trânsito.

A evolução natural das coisas, com o passar do tempo, torna o produto ou equipamento mais simples passível de armazenar cada vez mais informações e de modo mais inteligente, por meio de recursos avançados de interação e interface homem-máquina. Assim, , por meio da inclusão digital, o acesso a esses dispositivos são expandidos para diversas classes da sociedade. E devido a toda essa interação, acessibilidade, mobilidade e facilidade de transposição de conteúdo digital de diversos equipamentos torna a segurança da informação um desafio, para que seja mantido o sigilo dos dados do usuário titular de tais conteúdos *online*, os quais, agora, podem ser armazenados em uma *smart* TV, micro-ondas, uma geladeira, entre outros, objetos esses que interagem com outros usuários à sua volta, bem como com o próprio fabricante.

Mas o que vem a ser a IoT? A IoT (sigla do termo em inglês Internet of Things, ou, em português, Internet das Coisas) refere-se à capacidade de que objetos usados no cotidiano do ambiente real interliguem-se com a *internet*, de modo a comunicarem-se, reportar informações sobre seu estado e funcionamento. De modo geral, a IoT relaciona-se com a ampla gama de dispositivos conectados à *internet* passíveis de se comunicarem com outros dispositivos e redes, de captar e transmitir dados e receber e executar ordens.[29]

Campos Pataca cita[30] que a Internet das Coisas pode ser classificada como uma terceira geração da *internet* a que se está habituado hoje, também chamada de Web 3.0, a qual compreende a capacidade de os objetos também se conectarem com a *internet* e de se comunicarem tanto entre si quanto com máquinas e sistemas de informações, bem como com as pessoas. Enquanto a primeira geração foi aquela fundada na digitalização da informação, a segunda inseriu indivíduos, maciçamente, como criadores de conteúdos, sobretudo por meio das mídias sociais.

De forma básica e sem nos aprofundarmos nos significados mais técnicos, a arquitetura da IoT se divide em camadas, e cada uma possui função necessária ao funcionamento do sistema. Elas podem ter de três a cinco camadas, as quais,

[29] PATACA, 2021, p. 208.
[30] PATACA, 2021, p. 208.

de forma básica, são: camada de percepção, de rede e de aplicação. A primeira é a camada física, em que há sensores para detectar e coletar informações sobre o ambiente, bem como parâmetros físicos e identificar objetos inteligentes do ambiente. A segunda é a camada responsável pela conexão com outros objetos inteligentes, dispositivos de rede e servidores, usados também para transmissão e processamento de dados do sensor. A terceira camada é responsável pela entrega dos serviços específicos ao usuário, sendo definidas nesta as aplicações nas quais a IoT pode ser implantada, como em casas e cidades inteligentes, entre outros.[31]

Se divididas em cinco camadas, essas são definidas em: percepção, transporte, processamento, aplicação e camadas de negócios. A função das camadas de aplicação e percepção permanece a mesma da arquitetura com três camadas. Quanto às demais, essas possuem os seguintes papéis: a camada de transporte repassa dados do sensor da camada de percepção para camada de processamento e vice-versa, usando redes como Bluetooth, *wireless*, *near-field communication* (NFC) [comunicação por campo de proximidade], *radio frequency identification* (RFID) [identificação por radiofrequência] etc. A de processamento (também chamada de *middleware*) armazena, analisa e processa enormes quantidades de dados advindos da camada de transporte, pode gerenciar e fornecer diversos serviços para camadas inferiores, bem como possui tecnologias, como banco de dados, computação em nuvem e módulos de processamento de *big data*. A quinta e última camada é a camada de negócios que gerencia todo sistema IoT, abrange aplicativos, modelos de negócios e lucros e a privacidade dos usuários.[32]

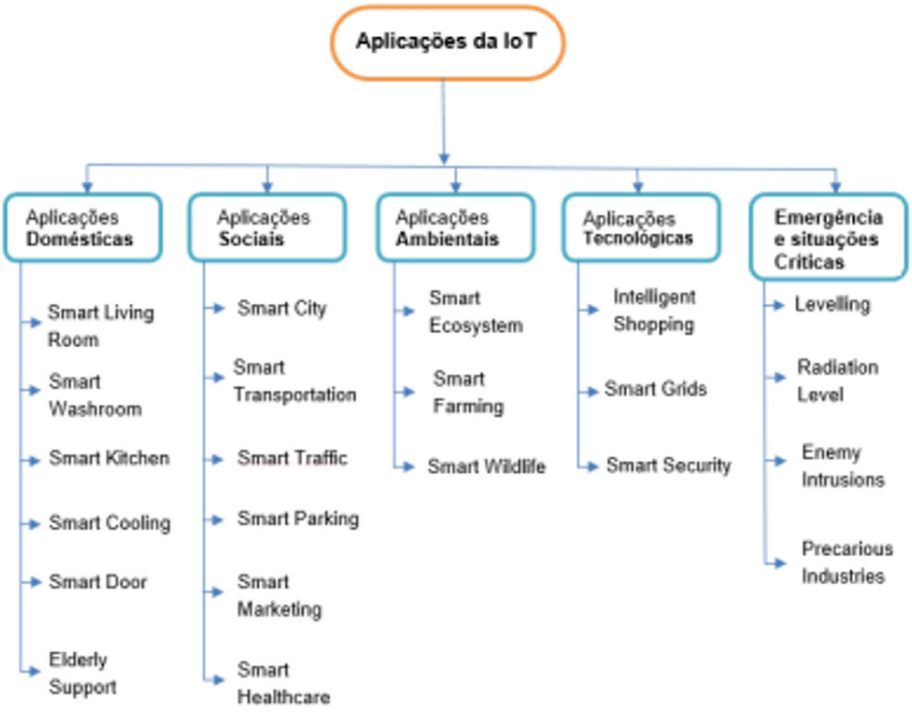
Quanto à comunicação da Internet das Coisas, essa utiliza, para tal, os protocolos de comunicação, os quais protegem e garantem a segurança dos dados trocados entre os dispositivos conectados. Geralmente, os dispositivos são conectados por meio de uma rede Internet Protocol (IP); entretanto, o Bluetooth e RFID, por exemplo, permitem que haja uma conexão local dos dispositivos, o que difere em potência, alcance e memória. Esses protocolos podem ser divididos, de forma ampla, em protocolos de rede e protocolos de dados. Os protocolos de dados IoT são utilizados para conectar dispositivos de baixa potência, fornecendo comunicação com o *hardware*, sem que haja conexão com a internet, usando uma rede com fio ou celular. São exemplos deles: Message Queuing Telemetry Transport (MQTT) [Transporte de Telemetria de Enfileiramento de Mensagens]; Constrained Application Protocol (CoAP) [Protocolo de Aplicação Restrita]; Advanced Message Queuing Protocol (AMQP) [Protocolo Avançado de Enfileiramento de Mensagens] etc. Já os protocolos de rede IoT são utilizados para conectar dispositivos via rede,

[31] SETHI; SARANGI, 2021, p. 2.
[32] SETHI; SARANGI, 2017, p. 3.

normalmente usados pela *internet*. São exemplos destes: *wi-fi*, Bluetooth, ZigBee, entre outros.[33]

De modo geral, a IoT é uma renovação tecnológica que, cada vez mais, contribuirá para otimização e automação de tarefas cotidianas e poderá trazer informações relevantes para benefício público e para empresas privadas, o que torna seus produtos e serviços prestados mais assertivos. Essa conexão virtual de dados, indivíduos, processos e coisas podem alcançar diversos domínios práticos, como domínio doméstico, social, ambiental, emergencial, incluídas aqui situações críticas e tecnológicas, conforme demonstra a figura a seguir:

Figura 1 - Principais áreas de aplicação da IoT



Fonte: *Revista de Direito, Estado e Telecomunicações* (2021).

Devido a toda essa conexão dos dispositivos IoT à rede, a segurança se torna a preocupação principal, uma vez que aumenta a possibilidade de ataques, *malwares* e invasões de *hackers*; trata-se de um risco potencial, mas sim um risco real. O crescimento e o uso da IoT dependem principalmente do aspecto de segurança,

[33] PATACA, 2021, p. 208.

uma vez que medidas de segurança devem controlar as ações tanto dos usuários quanto dos objetos. De modo paralelo, considerando-se que os dispositivos são caracterizados por recursos computacionais restritos, não basta a utilização de mecanismos de segurança convencionais, e, devido à heterogeneidade e às diversas interconexões dos dispositivos, gera-se uma grande quantidade de dados difíceis de gerenciar.

Os ataques que podem ocasionar a captação ou acesso aos dados dos usuários é a grande preocupação, uma vez que a rotina diária, dados gerais de saúde, hábitos, entre outros, são informações que podem ser inferidas até mesmo de dados não críticos. Nessa mesma linha, Allhoff e Henschke[34] abordam que, por meio dessa coleta de dados, é possível construir um perfil dos usuários, por exemplo, casas inteligentes, as quais podem mostrar rotina, hábitos de consumo e diversas informações, que muitas vezes são repassadas ao fabricante (nem sempre criptografadas). Isso demonstra que não apenas o mercado pode ter acesso a tais dados, mas *hackers* também podem fazer uso para fins nefastos.

De acordo com Barati,[35] as leis de proteção de dados surgiram com fundamento em fornecer o direito de privacidade de dados, de modo a não permitir que empresas que tratam dados os forneçam a outras empresas sem a devida permissão de seus titulares. Por essa razão, antes da realização do processamento de dados, a LGPD determina que haja o consentimento dos usuários, proibindo qualquer coleta de dados sem autorização e dando aos usuários pleno direito de manipular seus dados por meio de dispositivos inteligentes, ou por qualquer outro meio pelo qual possam acessar seus dados.

A Lei Geral de Proteção de Dados não traz definições quanto à proteção dos equipamentos, apenas faz alusão às boas práticas de segurança, deixando como responsabilidade do agente responsável controlar os dados a criação de mecanismos capazes de proteger os equipamentos. Podem eles criar normas de segurança, desenvolver os padrões técnicos, estabelecer métodos de supervisão dos dados, entre outros procedimentos técnicos e administrativos capazes de estabelecer um tratamento de acordo com a LGPD.

A criação e o uso de boas práticas de segurança de dados sempre foram recomendados; entretanto, requerem investimentos financeiros em recursos humanos e tecnológicos, o que[36] levou à sua adoção por poucas organizações. No entanto, a LGPD surgiu estabelecendo tais práticas em formato de lei, prevendo penalidades, como o recebimento de multas. A observação destas ainda é importante para evitar que haja vazamento de dados dos usuários. São diversos os setores em

[34] ALLHOFF; HENSCHKE, 2018, p. 59.
[35] BARATI, 2020.
[36] POHLMANN, 2020.

que pessoas mal-intencionadas invadem em busca de dados pessoais. Exemplo é a área da saúde, na qual os dados são alvo, pois podem ser vendidos na *dark web* com mais facilidade.[37]

Dessa forma, a interseção entre a privacidade e a IoT inicia-se por meio da percepção de que os dispositivos IoT podem coletar enormes quantidades de dados de seu usuário e de que esses dados são passíveis de serem analisados e compartilhados.[38] Exemplo foi o caso da Target,[39] amplamente divulgado, em que a empresa explorou hábitos de compra de determinada cliente, prevendo que esta estava gestante e enviando-lhe uma mala com diversos itens de bebê para sua residência. Ocorre que a usuária estava cursando o ensino médio e, embora estivesse grávida, sua família não tinha conhecimento do fato. Ou seja, a descoberta da gravidez se deu em razão da mala direta. A Target utilizou dados estatísticos por meio da análise de dados com base nas compras da cliente e, em pouco tempo, padrões úteis surgiram. Percebe-se, nesse caso, que a empresa estava coletando dados significativos da usuária, certamente vinculados ao seu cartão de crédito, e utilizou tais informações para traçar o perfil da cliente, prevendo, acertadamente, que ela estava grávida. A criação de perfil do usuário pode se mostrar uma boa prática de negócios, porém possivelmente invasiva, sem o consentimento do cliente.[40]

Logo, deve-se reconhecer que a IoT, devido a sua riqueza de sensores e comunicações integradas, oportuniza a reunião de um grande número de informações pessoais, a qual pode afetar, de forma significativa, a privacidade do indivíduo. Esse risco aumenta quando, junto à IoT, aplica-se a Inteligência Artificial.

A IA também possui capacidade de adquirir, processar e interpretar uma enorme quantidade de dados e decidir com base na interpretação destes dados. Considerando essa característica de coleta de dados, o que aumenta sua capacidade de observar o comportamento humano, há uma preocupação com relação à privacidade do indivíduo.[41]

Por meio da conectividade de vários sistemas de IA, que analisam dados e identificam *links* entre eles, a IA pode ser utilizada para transformá-los em grandes conjuntos de dados não mais anônimos, mesmo que não incluam dados pessoais por si mesmos.[42]

Assim, a IA passa a conseguir executar funções que antes apenas humanos conseguiriam, o que torna os indivíduos cada vez mais sujeitos às decisões ou

37 RILEY, 2019.
38 WEBER, 2015 citado por ALLHOFF; HENSCHKE, 2018, p. 58.
39 A Target é uma varejista de mercadorias em geral com lojas em todos os 50 estados dos EUA e no distrito de Columbia.
40 ALLHOFF; HENSCHKE, 2018, p. 58.
41 GABARDO; MENENGOLA; SANMIGUEL, 2023, p. 4.
42 GABARDO; MENENGOLA; SANMIGUEL, 2023, p. 5.

assistência da IA, as quais, por vezes, são difíceis de compreender e contestar, de forma eficaz, se necessário. O risco de tais decisões à sociedade se dá pela possibilidade de estas representarem, assim como nos humanos, discriminação, violação da privacidade, efeitos adversos nos processos democráticos e vigilância em massa (HEDLUND, 2022).[43]

Para proporcionar maior segurança jurídica aos usuários e desenvolvedores, é necessário regulamentação precisa que trate desses riscos e proteja os direitos e garantias fundamentais, uma vez que essa insegurança jurídica, consequência da ausência regulatória, pode prejudicar o uso da tecnologia e, com isso, causar danos irreversíveis aos que investem em IA.[44]

6 Caso iRobot – aquisição da iRobot pela Amazon

Um caso importante que envolve IoT foi a aquisição pela Amazon do iRobot, fabricante do robô aspirador Roomba.[45] Tais robôs são aspiradores que funcionam por meio de sensores que detectam obstáculos, escadas e paredes, além de medirem as distâncias em que devem trabalhar e possuírem tecnologia que os permite retornarem sozinhos aos seus locais de recarga, sem que seja necessário que o usuário realize algum comando.[46]

Os sensores de obstáculos ficam na parte do para-choque; o robô é capaz de identificar objetos pelo caminho, como mesas e cadeiras, desviando sem colidir com eles. Os sensores de escada (ou *cliff sensors*, para identificar "penhascos") são utilizados para evitar que o robô não se quebre em quedas, emitindo sinais infravermelhos pelo aspirador inteligente, que permanece todo tempo buscando identificar a superfície. Uma vez que não localize, imediatamente muda de direção. Da mesma forma, por meio de infravermelhos, detectam as paredes e conseguem acompanhar essas ao longo das bordas, mas em uma distância que evite o impacto.

Além dos sensores, o robô tem capacidade de mapear todos os ambientes da casa, o que auxilia o funcionamento do aspirador *smart*. Essa tecnologia integrada dos dispositivos utiliza câmeras digitais acopladas no dispositivo, ou *lasers* de detecção. Por meio de tais funcionalidades, coleta dados, combina informações e constrói algo parecido com um mapa mental do ambiente a ser limpo, sendo tal sistema também conhecido como Vision Simultaneos Localization and Mapping (VSLAM) [Localização Simultânea Visual e Mapeamento]. Assim, a função de limpeza do robô se torna mais eficiente e precisa, pois toda a planta do local

43 GABARDO; MENENGOLA; SANMIGUEL, 2023, p. 7.
44 EUROPEAN COMMISSION, 2020.
45 ALVES, 2022.
46 GIANTOMASO, 2018.

permanece armazenada no *software*, o que possibilita que o próprio equipamento defina trajetórias mais ordenadas, movendo-se em linhas retas.

Ainda, por meio da conexão via *wi-fi*, o robô é compatível com a Amazon, Alexa e Google Assistente, bem como é equipado com câmeras que permitem o mapeamento das casas (ou outros locais onde estejam), de modo a conhecer o tamanho dos cômodos e os móveis presentes em cada um, o que permite que a Amazon faça crescer seu grande banco de dados sobre comportamento humano.

Um dos *sites* que trouxe a notícia de tal aquisição e abordou as funcionalidades da tecnologia, o Yahoo Finanças, optou pelo título da matéria a seguinte frase: "Amazon compra empresa e fica ainda mais 'espiã'", citando ainda uma fala do CEO da iRobot em que este afirma que havia anunciado, em entrevista, que

> a última atualização de *software* do Roomba faria com que ele tivesse um conhecimento mais aprofundado do mapa da sua casa e dos seus hábitos. O robô, em vez de bater nas paredes constantemente, é capaz de memorizar onde os móveis e objetos de decoração estão de modo a eventualmente não colidir com nada, nem mesmo, com o seu dono.[47]

Com isso, a Amazon se tornou capaz de, por meio de dados adquiridos por tal dispositivo, ver dentro da residência daqueles que o adquirissem, tomando conhecimento da localização de cada cômodo da casa e dos móveis que nela estão, de possíveis obras em andamento e muito mais.

O Yahoo Finanças ainda expôs fala da diretora da divisão Alexa Smart Home, Marja Koopmans, para a qual a próxima fronteira na Inteligência Artificial não é mais informação, e sim mais contexto. Ela informou que o iRobot fornece resquícios desse contexto e, devido à utilização de armazenamento em nuvem, é capaz de compartilhar facilmente as informações com outros dispositivos. Nas palavras de Marja, "conseguimos entender a expressão 'vá para a cozinha e me pegue uma cerveja' por uma década. Mas se eu não sei onde fica a cozinha, e não sei onde fica a geladeira, e não sei como é uma cerveja, realmente não importa se eu entendo suas palavras".[48]

Verificada a capacidade do novo robô, o qual já está disponível no mercado, mostra-se válida uma abordagem não exaustiva da política de privacidade da empresa iRobot responsável pela criação do Roomba, bem como da política de privacidade adotada pela Amazon, a qual adquiriu a empresa e realiza a venda de tal equipamento.

47 AMAZON..., [2022a].
48 AMAZON..., [2022a].

A política de privacidade do iRobot estabelece que: 1) o controlador de dados, para fins das leis de proteção de dados aplicáveis, é o iRobot Corporation; 2) os dados coletados são informações do próprio usuário, de terceiros, de aplicativos e de alguns robôs; 2.1) as informações pessoais que o usuário fornece, como nome, *e-mail*, usuário e senha, histórico de compras, entre outros, também são armazenados, porém, separadamente dos dados do robô, desidentificados, com acesso restrito apenas a quem precisar; 3) a iRobot recebe informações de terceiros sobre o usuário, em situações em que o *login* realizado pelo titular dos dados é realizado por meio de rede social ou serviço de autenticação de terceiros, ou ainda podem adquirir tais informações quando ocorrer interação com as contas em rede social da empresa, por meio de ações como "curtir" ou "seguir". Essas mesmas informações são ainda utilizadas para que a iRobot consiga operar, manter e fornecer ao usuário recursos e as funcionalidades de seu serviço.[49]

Quanto ao robô, informam que: 1) sua tecnologia inteligente possibilita que transmitam dados sem fio para o serviço, os quais são armazenados em um estado desidentificado, separado das informações identificáveis; 2) ao registrar-se o robô, é armazenado o nome dado a ele pelo usuário, bem como as informações coletadas por este sobre o ambiente no qual é implantado, como sinal *wi-fi*, movimento do robô pelo ambiente, a fim de criar "mapa" do local de seu domínio, da existência e dos tipos de objeto (cadeira, mesa, geladeira, entre outros) ou obstáculos encontrados; 3) as imagens das câmeras dos robôs são coletadas a partir do consentimento do usuário; contudo, elas não ficarão visíveis à iRobot, apenas em caso em que, novamente, haja o consentimento do compartilhamento das imagens com a empresa; 4) as informações não são transmitidas pelos robôs enquanto não forem registrados *online* e conectados à rede *wi-fi* ou Bluetooth ou à *internet*, por qualquer outro método.[50]

Já a política de privacidade da Amazo volta-se ao comportamento do usuário quanto consumidor, de modo que estabelece o seguinte: 1) os dados informados são armazenados quando o usuário acessa o *site*, aplicativo ou outros serviços disponibilizados, sendo alguns opcionais e outros coletados de forma automática por meio dos *cookies*;[51] 2) ocorre compartilhamento de dados com terceiros em casos em que a Amazon entende que a liberação é apropriada ao cumprimento da lei, ou para executar as condições de uso e demais acordes, bem como para

[49] IROBOT CORPORATION, 2022.

[50] IROBOT CORPORATION, 2022.

[51] Os *cookies* são pequenos arquivos criados por sites visitados e que são salvos no computador do usuário, por meio do navegador. Estes armazenam diferentes informações e dados do usuário, como login, sua forma de navegar, quanto tempo permaneceu na página, que páginas do site foram visitadas e informações digitadas em algum formulário do *site*. *Cookies* são também comumente relacionados a casos de violação de privacidade na *web*.

proteger os direitos, propriedade ou segurança da Amazon, dos usuários ou terceiros, incluindo-se, aqui, a troca de informações com outras empresas e organizações para proteção de fraude e redução de riscos de crédito; 3) quanto ao acesso aos dados pelo usuário, o titular pode escolher não fornecer as informações, mesmo quando necessárias para realização da compra, e pode ainda adicionar ou atualizá-las, casos em que a Amazon conserva uma cópia da versão anterior em seu arquivo.[52]

Em ambas as políticas de privacidade, cita-se o necessário consentimento do usuário para que sejam os dados, em sua maioria, coletados, o que demonstra concordância com o texto legal da LGPD, o qual prevê tal consentimento, em seus arts. 5º, inciso XII, 7º, inciso I, e 14, inciso 1º. Entretanto, é evidente que, com o advento da IoT, ainda que seja ela arquitetada dentro das normas estabelecidas na LGPD, há uma mitigação do princípio da privacidade, se se considerar que sempre haverá vulnerabilidade nos dispositivos e uma enorme coleta de dados para o funcionamento deles, uma vez que, em sua essência, a IoT aplica algoritmos de Inteligência Artificial e ainda cruza informações por meio do *machine learning*, com a finalidade de gerar estatísticas capazes de detectar padrões e comportamentos dos usuários.

7 Conclusões

Conforme abordado anteriormente, a sociedade atual tem como seu elemento central a informação, tendo em vista o desenvolvimento do capitalismo, em que a informação assume cada vez mais um papel relevante, fazendo nascer uma nova forma de organização da sociedade, tanto no aspecto social quanto político e econômico. Nesse cenário, a informação tornou-se uma riqueza em todos os setores, intensificando-se no uso da tecnologia, a qual facilitou a coleta, produção, processamento, transmissão e armazenamento de dados.

Segundo a LGPD, todos os usuários possuem direito à privacidade e proteção de seus dados pessoais perante empresas públicas e privadas. Ocorre que tal contexto se mostra como um desafio à IoT, uma vez que tais dispositivos coletam uma gama de informações de seus usuários, aplicando algoritmos de inteligência artificial e cruzando tais informações de modo a gerar estatísticas capazes de detectar padrões no comportamento humano. Nesse contexto, os maiores desafios verificados da IoT são: adotar métodos para autorização da coleta do uso dos dados dos usuários pela empresa responsável; especificar padrões seguros para transmissão de dados; promover armazenamento seguro dos dados, bem como adotar procedimento que eliminem informações do usuário quando findada a relação

[52] AMAZON, [2022b].

entre este e a empresa prestadora do serviço. Isso considerando a capacidade restrita dos dispositivos IoT, tanto de memória como de processamento, uma vez que se trata de objetos do cotidiano.

Além disso, essa "onipresença" da IoT traz questionamentos significativos sobre a privacidade dos indivíduos e em como tratar essa diversidade de requisitos para segurança dos serviços. Isso demonstra o necessário desenvolvimento de soluções de segurança adaptáveis, centradas no usuário, como por meio do gerenciamento de perfis e políticas de segurança e de privacidade. Busca-se, assim, preservar a autonomia dos usuários, a fim de que estes permaneçam no controle de suas próprias informações.

Como um dos meios possíveis para se garantir a autonomia, pode-se pensar na adoção mais clara e efetiva das políticas de privacidade. Mas não uma política de privacidade impositiva, em que o indivíduo tem suas opções reduzidas apenas ao "aceito" ou "não aceito" tais termos, o que influencia a prestação do serviço de determinado equipamento. Mas sim adotar, por exemplo, o método de *checklist*, em que os tópicos sobre o tratamento dos dados, tantos os necessários ao funcionamento de determinado dispositivo quanto aqueles usados apenas para aperfeiçoar a prestação de serviços, poderiam ser lidos em tópicos e habilitados ou desabilitados pelo usuário, conforme sua preferência. Claro que os dados indispensáveis ao funcionamento do equipamento permaneceriam sendo coletados e tratados dentro da lei, o que deve aparecer de forma clara ao usuário; porém, aqueles dados não essenciais poderiam ter coleta desabilitada pelo usuário. Tal modelo de *checklist* ainda proporcionaria uma leitura mais agradável e menos cansativa ao indivíduo.

Ainda, tendo em vista as boas práticas de segurança, as quais a LGPD buscou prever, bem como ocorre com a Regulamento Geral de Proteção de Dados (RGPD) aplicado na Europa, cita-se aqui a importância da adoção do *privacy by design* e do *privacy by default*, os quais destacam a importância de ser considerada a privacidade desde os estágios iniciais do *design* e durante todo o processo de desenvolvimento do produto, do serviço e dos processos que envolverão o tratamento dos dados pessoais e, junto ao *design*, considerar também as opções que o sistema ou serviço disponibilizarão ao indivíduo, demonstrando a quantidade de dados pessoais que serão por ele compartilhados, devendo ser as configurações padrão as mais favoráveis à privacidade.[53]

A insuficiência do espectro normativo analógico como função ordenadora capaz de conceder respostas aos problemas, ora referenciado, reivindica uma

[53] ALVES; PEIXOTO; ROSA, 2021, p. 13.

construção teórica robusta e intensa sobre a regulação digital, capaz de definir um regime jurídico próprio, instrumentos de cautela e prevenção contra uso inadequado e antidemocrático dos dados, plataformas e máquinas robôs para direcionamento de escolhas públicas e privadas.[54]

Com isso, verifica-se a necessidade de regulamentação dos procedimentos de segurança a serem aplicados pelos responsáveis pelo tratamento dos dados pessoais, a fim de que haja garantia da integridade, da disponibilidade, da autenticidade, do sigilo das informações, sendo esses os quatro pilares da segurança da informação, os quais devem ser observados junto aos princípios relacionados à proteção dos dados pessoais, bem como dos direitos resguardados aos titulares dos dados, como os direitos à oposição, à informação, ao acesso e à eliminação.

Referências

ALLHOFF, Fritz; HENSCHKE, Adam. The Internet of Things: foundational ethical issues. *Internet Of Things*, v. 1-2, p. 55-66, set. 2018. DOI: http://dx.doi.org/10.1016/j.iot.2018.08.005.

AMAZON compra empresa e fica ainda mais 'espiã'. *Yahoo! Finanças*, [2022a]. Disponível em: https://br.financas.yahoo.com/noticias/amazon-quer-espionar-dentro-de-sua-casa-231348602.html?_guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADgR39pmzRQ_Azs9kGp5mTN4E5BbjJ4YCiBt8_tq8A5DgksR_isyVbdS4Bz7iFTJPgbLNA4mjS5HBYaBMIc8ctQ1xD5oTjcVdWZbUSX5YD89JWI2_npX5ikq-886qa2ufM0hzKnFgHRobR3f8rWyi2mGIkvuBijggZOzmczf3HwG&guccounter=2. Acesso em: 30 out. 2022.

AMAZON. Notificação de Privacidade da Amazon, [2022b]. Disponível em: https://www.amazon.com.br/hz/cs/help?nodeId=GX7NJQ4ZB8MHFRNJ. Acesso em: 30 out. 2022.

ALVES, David; PEIXOTO, Mario; ROSA, Thiago. *Internet Das Coisas (IoT)*: segurança e privacidade dos dados pessoais. Rio de Janeiro: Alta Books, 2021. 256 p.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. *Revista de Investigações Constitucionais*, v. 4, n. 3, p. 167-200, set./dez. 2017.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019. 328 p.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. São Paulo: Grupo GEN, 2021. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 29 out. 2022.

BRASIL. Decreto nº 592, de 6 de julho de 1992. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Pacto Internacional Sobre Direitos Civis e Políticos. *Diário Oficial da União*: Brasília, DF, 6 jul. 1992a. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 01 out. 2022.

[54] VALLE; GALLO, 2020, p. 78.

BRASIL. Decreto nº 678, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Convenção Americana Sobre Direitos Humanos. *Diário Oficial da União*: Brasília, DF, 9 nov. 1992b. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 01 out. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09 set. 2022.

BRASIL. Ministério Público Federal. Secretaria de Cooperação Internacional. *Tratados de direitos humanos*: Sistema Internacional de Proteção aos Direitos Humanos. Convenção Europeia para a Proteção dos Direitos humanos e das Liberdades Fundamentais, v. 4, Brasília, 2016.

BARATI, Masoud *et al*. GDPR Compliance Verification in Internet of Things. *IEEE Access*, v. 8, 29 jun. 2020. Disponível em: https://ieeexplore.ieee.org/document/9127459. Acesso em: 22 out. 2022.

CASTELLS, Manuel. *A sociedade em rede*. Tradução: Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 2013. 355 p.

COUNCIL OF EUROPE. Europe Court of Human Rights. *Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais* (1950), 4 nov. 1950. Disponível em: https://www.echr.coe.int/documents/d/echr/convention_por. Acesso em 07 set. 2022.

CRISTÓVAM, José Sérgio da Silva; HAHN, Tatiana Meinhart. Administração pública Orientada por Dados: Governo Aberto e Infraestrutura Nacional de Dados Abertos. *Revista de Direito Administrativo e Gestão Pública*, v. 6, n. 1, p. 1-24, jan./jun. 2020. DOI: http://dx.doi.org/10.26668/IndexLawJournals/2526-0073/2020.v6i1.6388.

EUROPEAN UNION. *Charter Of Fundamental Rights Of The European Union*, 7 dez. 2000. Disponível em: http://data.europa.eu/eli/treaty/char_2016/oj. Acesso em: 7 set. 2022.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da* USP, São Paulo, v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 25 out. 2022.

FROM, Danieli Aparecida; REZENDE, Denis Alcides. Modelo de Prestação de Serviços Públicos Municipais Conectados por meio da Internet das Coisas no Contexto da Cidade Digital Estratégica. *Contribuciones A Las Ciencias Sociales*, p. 15-28, 6 jul. 2021.

FORNASIER, Mateus de Oliveira. A aplicabilidade da Internet das Coisas (IoT) entre os direitos fundamentais à saúde e à privacidade. *Revista de Investigações Constitucionais*, Curitiba, v. 6, n. 2, p. 297-321, maio/ago. 2019.

FINANÇAS, Redação. Amazon compra empresa e fica ainda mais 'espiã'. *Yahoo Finanças*, 7 ago. 2022. Disponível em: https://br.financas.yahoo.com/noticias/amazon-quer-espionar-dentro-de-sua-casa-231348602.html?guccounter. Acesso em: 23 out. 2022.

GABARDO, Emerson; MENENGOLA, Everton; SANMIGUEL, Nancy Nelly González. A proposta europeia de regulação da Inteligência Artificial. *Sequência Estudos Jurídicos e Políticos*, v. 43, n. 91, 2023. DOI: 10.5007/2177-7055.2022.e91435. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/91435. Acesso em: 15 abr. 2023.

GARCIA, Rafael de Deus. Os direitos à privacidade e à intimidade: origem, distinção e dimensões. *Revista da Faculdade de Direito do Sul de Minas*, Pouso Alegre, v. 34, n. 1, p. 1-26, 2018. Disponível em: https://revista.fdsm.edu.br/index.php/revistafdsm/article/view/257. Acesso em: 24 out. 2022.

GONET BRANCO, Paulo Gustavo. Direitos fundamentais em espécie. *In:* GONET BRANCO, Paulo Gustavo. *Curso de direito constitucional*. 4. ed. São Paulo: Saraiva, 2009.

GIANTOMASO, Isabela. Entenda como funciona a tecnologia do robô aspirador de pó. *Techtudo*, 5 jul. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/07/entenda-como-funciona-a-tecnologia-do-robo-aspirador-de-po.ghtml. Acesso em: 23 out. 2022.

IROBOT CORPORATION. Política de Privacidade. *iRobot*, 2022. Disponível em: https://www.irobot.com.br/Legal/Privacy-Policy. Acesso em: 30 out. 2022.

LAFER, Celso. *A reconstrução dos direitos humanos um diálogo com o pensamento de Hannah Arendt*. São Paulo: Schwarcz, 1991. 406 p. Disponível em: https://mpassosbr.files.wordpress.com/2013/03/a-reconstruc3a7c3a3o-dos-direitos-humanos-celso-lafer.pdf. Acesso em: 28 set. 2022.

MOREIRA, Egon Bockmann. Direitos Fundamentais para Humanos Digitais. *Gazeta do Povo*, 19 ago. 2019. Disponível em: https://www.gazetadopovo.com.br/vozes/egon-bockmann-moreira/direitos-fundamentais-para-humanos-digitais/. Acesso em: 5 outubro de 2022.

PATACA, Campos Calenga. A Internet das Coisas: Tipologias, Protocolos e Aplicações. *The Law, State and Telecommunications Review*, v. 13, n. 2, p. 198-220, 2021. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/32773. Acesso em: 22 out. 2022.

PORTELA, Irene Maria; MOTTA, Ivan Dias da; ABAGGE, Yasmine de Resende. O uso dos dados pessoais nas políticas públicas de combate à covid-19. *Revista Jurídica*, v. 4, n. 61, p. 70-90, out. 2020. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/4478/371372683. Acesso em: 15 out. 2022.

SCHERMER, Bart Willem. *Software agents, surveillance, and the right to privacy*: a legislative framework for agent-enabled surveillance. Leiden: Imprensa da Universidade de Leiden, 2007. 241 p. Disponível em: https://hdl.handle.net/1887/21094. Acesso em: 10 out. 2022.

SILVA, Daniel Pereira Militão. *Desafios do ensino jurídico na pós-modernidade*: da sociedade agrícola e industrial para a sociedade da informação. 2009. 280 f. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2009.

SPIECKER DE OLIVEIRA, Nairobi *et al*. Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). *Revista Eletrônica de Iniciação Científica em Computação*, São Leopoldo, v. 17, n. 4, 2019. Disponível em: https://seer.ufrgs.br/reic/article/view/88790. Acesso em: 09 out. 2022.

SETHI, Pallavi; SARANGI, Smruti R. Internet of Things: architectures, protocols, and applications. *Journal Of Electrical and Computer Engineering*, v. 2017, p. 1-25, 2017.

URQUHART, Lachlan; LODGE, Tom; CRABTREE, Andy. Demonstrably doing accountability in the internet of things. *International Journal of Law and Information Technology*, v. 27, n. 1, p. 1-27, 2019. DOI: https://doi.org/10.1093/ijlit/eay015.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2007. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.D76AACD6&lang=pt-br&site=eds-live. Acesso em: 3 out. 2022.

VALLE, Vivian Cristina Lima López; GALLO, William Ivan. Inteligência Artificial e Capacidades Regulatórias do Estado no Ambiente da administração pública Digital. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, v. 20, n. 82, p. 67-86, out./dez. 2020

ZANETTI DE OLIVEIRA, Dânton Hilário; FREITAS, Cinthia Obladen de Almendra. *Big Data e os limites à livre iniciativa no âmbito da Lei Geral de Proteção de Dados Pessoais.* 2022. 198 f. Dissertação (Mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2022. Disponível em: https://archivum.grupomarista.org.br/pergamumweb/vinculos/0000a6/0000a635.pdf. Acesso em: 3 out. 2022.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

VALLE, Vivian Lima López; BARBOSA, Bruna Gavron. Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT. *International Journal of Digital Law*, Belo Horizonte, ano 4, n. 1, p. 35-61, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.valle.

Diretrizes para Autores

1. Submissão de artigos
As propostas de artigos para publicação na *International Journal of Digital Law* deverão ser enviadas através do sistema eletrônico de submissões (gratuitamente), por meio de cadastro no Sistema Eletrônico e acesso mediante login e senha a ser realizado no site. Não serão aceitas propostas enviadas por e-mail. A revista reserva-se o direito de aceitar ou rejeitar qualquer original recebido, de acordo com as recomendações do seu corpo editorial, inclusive por inadequação da temática do artigo ao perfil editorial da revista, como também o direito de propor eventuais alterações.

2. Qualificação dos autores
Ao menos um dos autores do artigo deverá possuir o título de Doutor (Dr.), Doctor of Juridical Science (J.S.D. ou S.J.D.), Doctor juris (Dr. iur. ou Dr. jur.), Doctor of Philosophy (Ph.D.) ou Legum Doctor (LL.D.). A exigência poderá ser relativizada, nunca extrapolando o percentual de 30% por edição, em casos excepcionais de: (i) artigos de autores afiliados a instituições estrangeiras; (ii) artigos escritos em inglês.

3. Ineditismo e exclusividade
Os textos para publicação na *International Journal of Digital Law* deverão ser inéditos e para publicação exclusiva, salvo no caso de artigos em língua estrangeira que tenham sido publicados fora do país. Uma vez publicados nesta revista, também poderão sê-lo em livros e coletâneas, desde que citada a publicação original. Roga-se aos autores o compromisso de não publicação em outras revistas e periódicos, bem como de que as propostas de artigo não se encontrem postulados de forma simultânea em outras revistas ou órgãos editoriais.

4. Idiomas
Podem ser submetidos artigos redigidos em Português, Espanhol ou Inglês.

5. Cadastro dos metadados no sistema eletrônico de submissões
5.1. No momento da submissão do artigo no sistema eletrônico, os campos dos metadados deverão ser preenchidos obrigatoriamente de acordo com estas diretrizes, sob pena de rejeição liminar da submissão.
5.2. Autores
5.2.1. *Nome/Nome do Meio/Sobrenome:* indicação do nome completo do(s) autor(es) apenas com as iniciais de cada nome em caixa alta. Em caso de artigos em coautoria, os nomes de todos os coautores devem ser inseridos no sistema na ordem que deverá constar no momento da publicação.
5.2.2. *E-mail:* indicação do e-mail do(s) autor(es) para contato, que será obrigatoriamente divulgado na versão publicada do artigo.
5.2.3. *ORCID iD:* indicação do número de identificação ORCID (para maiores informações clique aqui). O identificador ORCID pode ser obtido no registro ORCID. Você deve aceitar os padrões para apresentação de iD ORCID e incluir a URL completa; por exemplo: https://orcid.org/0000-0003-1781-1726.