



# REVISTA CIENTÍFICA

**CAMPUS PARTY**

**CPG01AS3**



**REVISTA  
CIENTÍFICA  
CAMPUS PARTY**



## O Desenvolvedor Lebre e o Desenvolvedor Tartaruga - uma Fábula Moderna

Esses dias eu vi um desenvolvedor falando de um projeto que ele supervisionou, como uma experiência para decidir que caminho seguir.

Ele contratou:

um desenvolvedor experiente (19 anos de experiência)

e um dev novato (4 anos de experiência)

Para fazer um mesmo projeto, um MVP (Minimum Viable Product).

O experiente fez o projeto somente codificando.

O novato fez o projeto codificando e usando ferramentas de no-code e inteligência artificial.

Resultado?

No período alocado para o projeto,

O novato fez o projeto inteiro em apenas uma semana.

O experiente fez apenas 7% do projeto.

Uau...

(Imagino você pensando...)

Acabou o espaço para desenvolvedores, a inteligência artificial vai tomar conta de tudo!

É uma forma de ver a coisa toda.

Como eu vejo?

Existe cada vez MAIS espaço e oportunidades para você, desenvolvedor de software!

Primeiro porque o “novato” era alguém com 4 anos de experiência. Considerando que leva cerca de 3 anos para você desenvolver o seu cérebro de desenvolvedor, ele até podia ser um “novato” comparado com o outro, mas era um profissional que sabia o que estava fazendo. Eu não conheço pessoalmente esse desenvolvedor da experiência, mas tenho mentores meus que, com 4-5 anos de carreira, são profissionais sênior bem qualificados. Acredito que seja o caso aqui.

Além disso, é importante observar que a “inteligência artificial” não desenvolveu o projeto sozinha. Na verdade, não fez nada sozinha! Quem desenvolveu foi um profissional, capaz de entender os requerimentos, tomar decisões, escolher alternativas, e, em especial, capaz de usar e direcionar as ferramentas para o resultado desejado pela empresa.

Outra coisa importante é a capacidade de entender o seu valor no processo. Uma coisa que me chamou atenção no projeto mencionado acima foi que o desenvolvedor experiente achou que fazendo o código todo na mão ele traria melhores resultados, porque o custo de rodar o software seria menor e a empresa teria todo o controle da solução, em vez de ser um software que dependia de serviços de no-code. Além disso, pela descrição do projeto, pode ser que ele tenha considerado que o custo de usar as ferramentas de inteligência artificial encareceria o processo de desenvolvimento.

Tudo isso na verdade REDUZIU o valor dele no projeto! Porque no final, ele entregaria o projeto 13 vezes mais lento, e o valor do tempo dele aumentaria o custo do projeto em 25 vezes!

Ou seja, ao tentar otimizar por algo que não era o resultado buscado pela empresa, ele reduziu o próprio valor. E cá entre nós: você preferiria ficar 13 vezes mais tempo preso a um projeto, em vez de entregar logo e partir para algo mais desafiador?

Do jeito que eu vejo, essa é uma versão moderna da Fábula da Lebre e da Tartaruga.

O desenvolvedor experiente – a lebre – ficou complacente. Achou que seus conhecimentos seriam suficientes para que ele continuasse no topo e ganhasse a corrida. Com isso, ele passou muito tempo curtindo a própria experiência e pensando no próprio valor, que acabou dormindo no ponto. Enquanto isso, o desenvolvedor novato – a tartaruga – colocou o foco em cruzar a linha de chegada, focou no resultado esperado pela empresa. Usou todas as ferramentas que pode, e quando o experiente acordou, ele já tinha entregue o projeto, e já estava contratado pela empresa.

O que nos leva a você e sua carreira. Essa história nos mostra:

- **Foco.** Muitos desenvolvedores pensam que o seu foco é a tecnologia que você sabe. Mas não. Foco é o resultado, é o problema que você resolve.

Experiência. Desenvolver software é uma atividade criativa que exige experiência. Por mais que você possa usar ferramentas para acelerar seu trabalho, é a sua capacidade de tomar decisões e fazer escolhas que vai te colocar nas melhores posições.

- **Ferramentas.** Ficar antenado com as ferramentas existentes é sinal de experiência. Ferramentas não substituem pessoas. Ferramentas tornam pessoas mais eficientes. Pessoas mais eficientes substituem pessoas menos eficientes...

- **Habilidades.** Não basta ter anos de experiência se você não está sempre afinando suas habilidades. E habilidades são afiadas quando você faz e aplica suas habilidades em algo real, trazendo resultado para as pessoas (e empresas) a sua volta.

- **Trade-off e resolução de problemas.** Desenvolvedores não são escrevedores de código. Há décadas que sabemos que qualquer ferramenta faz isso. Desenvolvedores são resolvidores de problemas. E para resolver problemas, você precisa tomar decisões e escolher as melhores opções dependendo das necessidades.

**Resultado.** Não existe foco, nem trade-off, nem mesmo a escolha das ferramentas se você não sabe onde quer chegar. Tenha clareza no resultado, e encontre os melhores caminhos para alcançá-los.

Se tem uma coisa que vai mudar a sua carreira, é ter foco no resultado. Eu acredito que você pode aprofundar suas habilidades, para que você crie seus próprios caminhos na sua carreira técnica. É por isso que o meu foco é te ajudar a identificar e focar nos seus resultados. Porque você pode codar no seu trabalho, pra se divertir, e até para conhecer amigos. Então, venha codar pra vida, venha para a Code4.Life - <https://code4.life>.

Bruno Souza

Desde 1995 Bruno ajuda desenvolvedores de software a crescer na carreira e a trabalhar em projetos fantásticos com times excelentes. Embaixador da Campus Party e coordenador do palco Campus Jobs, Bruno é Evangelista Java, presidente da Sociedade de Usuários Java, SouJava, e criador do projeto <https://code4.life>, onde discute a Carreira do Desenvolvedor de Software.

**THE IMPORTANCE OF GENDER DIVERSITY IN THE INNOVATION ECOSYSTEM: A STUDY OF WOMEN ENTREPRENEUR COMMUNITIES**

**A IMPORTÂNCIA DA DIVERSIDADE DE GÊNERO NO ECOSISTEMA DE INOVAÇÃO: UM ESTUDO DAS COMUNIDADES DE MULHERES EMPREENDEDORAS**

[Douglas Araújo Falcão .....07](#)

**EDUCAÇÃO EMPREENDEDORA E SEUS IMPACTOS NO CRESCIMENTO DO EMPREENDEDORISMO DE OPORTUNIDADE**

[Marília Marques Abreu, Katiana Ferreira Dos Reis Boaz, Jéssica Campos Souza.....17](#)

**INTERNET DAS COISAS VERSUS LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UM CONFRONTO EM PROL DA SEGURANÇA E DOS DIREITOS FUNDAMENTAIS.**

[Geisiana Campos Souza, Geana Campos Souza, Virgílio Norberto de Jesus Neto .....21](#)

**Abordagem YOLOv5 para Detecção e Classificação de Esferas de Solda no Encapsulamento de Semicondutores**

[Paulo Vitor Libório Pereira .....36](#)

**DIREITO FUNDAMENTAL À PRIVACIDADE E À PROTEÇÃO DOS DADOS PESSOAIS: UMA ANÁLISE FRENTE AO DESENVOLVIMENTO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL**

[Rebeca de Lima Nogueira .....46](#)

**UBERIZAÇÃO DO TRABALHO E JUVENTUDE: UMA DISCUSSÃO ACERCA DA SOCIOLOGIA DO TRABALHO**

[Vinicius Oliveira Seabra Guimarães .....60](#)

# THE IMPORTANCE OF GENDER DIVERSITY IN THE INNOVATION ECOSYSTEM: A STUDY OF WOMEN ENTREPRENEUR COMMUNITIES

## A IMPORTÂNCIA DA DIVERSIDADE DE GÊNERO NO ECOSISTEMA DE INOVAÇÃO: UM ESTUDO DAS COMUNIDADES DE MULHERES EMPREENDEDORAS

**Abstract.** The objective of this research work is to analyze the relationship between the innovation ecosystem and women's social changes. Although female leadership can be a crucial factor in promoting significant and sustainable changes in society, women face significant challenges in fully and equally participating in areas such as innovation and leadership. The research aims to understand how the innovation ecosystem can influence the success of women-led social change projects and identify the factors that encourage or hinder women's participation in the innovation ecosystem. Innovation ecosystems are defined as complex and dynamic groups of actors, resources, and institutions that interact to create, disseminate, and use new knowledge and technologies. The inclusion of women in these ecosystems is crucial to promoting diversity and innovation. However, women continue to face significant challenges in participating in innovation ecosystems and entrepreneurship, such as a lack of capital, mentoring, and support networks. The research aims to contribute to the development of more effective policies and strategies to promote gender equality and social justice.

**Keywords:** Innovation ecosystem, Female leadership, Women's communities, Inclusion, Diversity.

### **Resumo.**

O objetivo deste trabalho de pesquisa é analisar a relação entre o ecossistema de inovação e as mudanças sociais das mulheres. Embora a liderança feminina possa ser um fator crucial na promoção de mudanças significativas e sustentáveis na sociedade, as mulheres enfrentam desafios significativos para participar plena e igualmente em áreas como inovação e liderança. O objetivo da pesquisa é entender como o ecossistema de inovação pode influenciar o sucesso de projetos de mudança social liderados por mulheres e identificar os fatores que incentivam ou impedem a participação das mulheres no ecossistema de inovação. Ecossistemas de inovação são definidos como grupos complexos e dinâmicos de atores, recursos e instituições que interagem para criar, disseminar e usar novos conhecimentos e tecnologias. A inclusão de mulheres nesses ecossistemas é fundamental para promover a diversidade e a inovação. No entanto, as mulheres continuam a enfrentar desafios significativos na

participação em ecossistemas de inovação e empreendedorismo, como a falta de capital, mentoria e redes de apoio. O objetivo da pesquisa é contribuir para o desenvolvimento de políticas e estratégias mais eficazes para promover a igualdade de gênero e a justiça social.

Palavras-chave: Ecossistema de inovação, Liderança feminina, Comunidades de Mulheres, Inclusão, Diversidade

## 1. Introdução/Justificativa

A participação plena e igualitária das mulheres é essencial para alcançar a igualdade de gênero e promover o desenvolvimento sustentável (ONU Mulheres, 2021). No entanto, as meninas ainda enfrentam desafios significantes em sua participação em ecossistemas de inovação e liderança.

A relação entre o ecossistema de inovação e a transformação social encabeçada por mulheres é de grande importância, uma vez que a liderança feminina pode ser um fator crucial na promoção de mudanças significantes e duradouros na sociedade (Steinem, 2016).

Nos últimos anos, a proporção de mulheres em vários setores da sociedade, como política, educação, ciência e ambiente de negócios, aumentou gradualmente. Segundo o estudo de Farah (2004), essas mudanças foram resultado de movimentos que surgiram nos esforços para combater

a desigualdade entre homens e mulheres e aumentar a participação das mulheres em setores importantes da sociedade. Ao mesmo tempo, o processo de globalização das últimas décadas teve um grande impacto na mudança dos modelos sociais e econômicos de muitas nações, o que, segundo as conclusões de Castells (1999), levou a uma nova economia global baseada na tecnologia. Para alcançar a sustentabilidade, é importante que vários grupos sociais participem desse processo de crescimento, que também inclui a participação ativa das mulheres.

A relevância deste estudo decorre da necessidade de entender como os ecossistemas de inovação podem influir o sucesso de iniciativas de mudança social lideradas por meninas. Além disso, uma melhor compreensão dos fatores que promovem ou dificultam a participação das mulheres nos ecossistemas de inovação pode ajudar a desenvolver políticas e estratégias mais eficazes para promover a igualdade de gênero e a justiça social.

## Objetivo

O objetivo deste artigo é analisar a relação entre o ecossistema de inovação e a mudança social das mulheres. A liderança das mulheres pode ser um fator decisivo para provocar mudanças significativas e sustentáveis na sociedade, mas as mulheres enfrentam grandes desafios se quiserem participar plena e igualmente,

por exemplo, na inovação e na liderança. O objetivo da pesquisa é entender como o ecossistema de inovação pode influenciar o sucesso de projetos de mudança social liderados por mulheres e identificar fatores que incentivam ou dificultam a participação de mulheres no ecossistema de inovação. Espera-se que os resultados deste estudo contribuam para o desenvolvimento de políticas e estratégias mais eficazes para promover a igualdade de gênero e a justiça social.

Para dar conta deste estudo de caso o artigo está dividido em três partes. A parte inicial abarca as relações entre o ecossistema de inovação e o empreendedorismo feminino. Posteriormente se apresenta a metodologia do trabalho, e ao final se faz um panorama da participação feminina no Ecossistema de Inovação.

## **OS ECOSISTEMAS DE INOVAÇÃO E O EMPREENDEDORISMO FEMININO**

Os ecossistemas de inovação desempenham um papel importante no desenvolvimento de negócios e inovações liderados por mulheres. Segundo Freire e Guerra (2020), os ecossistemas de inovação podem ser entendidos como “grupos complexos e dinâmicos de atores, recursos e instituições que interagem e se influenciam para criar, disseminar e usar novos conhecimentos e tecnologias”.

Apesar de sua importância,

as mulheres continuam enfrentando desafios significativos para participar de ecossistemas de inovação e empreendedorismo. Conforme observado por Galbraith e Vickers (2019), “embora existam muitas iniciativas promissoras para promover o empreendedorismo feminino, o acesso a capital, mentoring e redes de apoio continuam carentes em termos de investimento e apoio”.

Além disso, a falta de diversidade nos ecossistemas de inovação pode limitar a criatividade e a inovação. Segundo Mahajan e Lundberg (2019), “a diversidade é essencial para a inovação porque incentiva ideias únicas e perspectivas diferentes”. Portanto, a inclusão de mulheres em ecossistemas de inovação é crucial para promover a diversidade e a inovação. No entanto, a inclusão de mulheres em ecossistemas de inovação não é importante apenas para promover a igualdade de gênero e a justiça social, mas também pode trazer benefícios econômicos. De acordo com um relatório do Banco Mundial (2019), o empreendedorismo feminino pode contribuir para o crescimento econômico e a redução da pobreza, criar empregos e inovar em setores sub-representados. Portanto, promover a participação de mulheres em ecossistemas de inovação pode ser uma estratégia econômica viável. Em suma, pode-se afirmar que os ecossistemas de inovação desempenham um papel importante no desenvolvimento do empreendedorismo feminino e na

promoção da igualdade de gênero e justiça social. No entanto, os desafios de inclusão e diversidade ainda precisam ser superados. Investir em políticas e estratégias que promovam a participação das mulheres nos ecossistemas de inovação pode beneficiar tanto as mulheres quanto a economia como um todo.

## COMUNIDADES DE MULHERES E SUA IMPORTÂNCIA NO ECOSSITEMA DE INOVAÇÃO

Uma forma de fortalecer a participação das mulheres no ecossistema de inovação é criar comunidades de mulheres empreendedoras. Segundo estudo de Gupta e Krishnan (2021), essas comunidades podem desempenhar um papel fundamental na promoção de redes de apoio, no compartilhamento de recursos e no empoderamento de mulheres empreendedoras. Segundo Lerner e Almeida (2020), essas comunidades são importantes porque fornecem um espaço seguro para as mulheres se conectarem e compartilharem experiências, desafios e oportunidades.

Além disso, as comunidades de mulheres empresárias podem ajudar a reduzir a sensação de isolamento que muitas vezes afeta as mulheres empresárias. Outra vantagem das comunidades empreendedoras de mulheres é que elas podem fornecer recursos e informações específicas para as necessidades das mulheres empreendedoras.

Por exemplo, a comunidade Girls in

Tech, fundada por Adriana Gascoigne em 2007, visa oferecer oportunidades e recursos para mulheres em tecnologia e empreendedorismo e promover a diversidade e inclusão na indústria. Além disso, a criação de comunidades de mulheres empreendedoras pode ajudar a mudar a cultura de inovação para uma direção mais inclusiva e diversificada. Como argumentam Gupta e Krishnan (2021), essas comunidades podem ser um catalisador para a mudança da indústria, promovendo a diversidade e a inclusão em todos os níveis. Em todo o Brasil existem comunidades que apoiam mulheres, algumas foram mapeadas no Quadro 1.

Quadro 01: Comunidades de Inovação e Empreendedorismo Feminino

Comunidade	Data de Fundação	Estado
Girls in Tech Brasil	2007	SP
Rede Mulher Empreendedora	2000	SP
Women in Tech	2015	RJ
Women Who Code	2011	SP
Lady Boss	2016	PR
Liga Empreendedoras	2020	BA
Mulheres de Produto	2017	SP
Rede de Mulheres Líderes Empreendedoras	2019	MG
Ladies That UX	2019	GO
Planeta Mulher	Informação Indisponível	GO
WTM - Women Techmakers	Informação Indisponível	GO
MulheresGO	2019	GO
Women in Blockchain Brasil	Informação Indisponível	SP

Fonte: Elaboração própria

Portanto, construir comunidades de mulheres empreendedoras é essencial para construir um ecossistema de inovação mais inclusivo e diversificado. Essas comunidades podem fornecer apoio, compartilhamento de recursos e capacitação para mulheres empresárias e promover a mudança cultural necessária para criar um ambiente de inovação verdadeiramente inclusivo.

## **A RELAÇÃO ENTRE O ECOSISTEMA DE EMPREENDEDORISMO, INOVAÇÃO E A TRANSFORMAÇÃO SOCIAL LIDERADA POR MULHERES**

A conexão do ecossistema de inovação com a mudança social protagonizada por mulheres é um tema cada vez mais importante na sociedade atual. A participação das mulheres em, entre outras coisas, inovação e liderança tem sido um desafio significativo, embora sejam importantes como promotoras de mudanças significativas e sustentáveis na sociedade.

É válido analisar a relação entre o ecossistema de inovação e a mudança social das mulheres, entender como o ecossistema pode influenciar o sucesso de projetos de mudança social liderados por mulheres e descobrir os fatores que incentivam ou dificultam a participação feminina. Ecossistemas de inovação são definidos como grupos

complexos e dinâmicos de atores, recursos e instituições que interagem para criar, disseminar e usar novos conhecimentos e tecnologias.

A inclusão de mulheres nesses ecossistemas é fundamental para promover a diversidade e a inovação. De acordo com Welter et al. (2018), a inclusão de mulheres em ecossistemas de inovação é essencial para promover a diversidade e a inovação. No entanto, as mulheres enfrentam desafios significativos para participar de ecossistemas de inovação e empreendedorismo, como falta de capital, mentoria e redes de apoio.

Nesse sentido, é importante criar políticas e estratégias para promover a igualdade de gênero e a justiça social para garantir a plena participação das mulheres em áreas como inovação e liderança. Outro estudo importante é o de Santos et al. (2021), que enfatiza a importância da liderança feminina na promoção de mudanças significativas e sustentáveis na sociedade. Segundo os autores, as mulheres desempenham um papel fundamental na mudança social, e a inovação pode ser uma ferramenta eficaz para atingir esse objetivo. No entanto, é necessário garantir que as mulheres recebam as ferramentas e oportunidades necessárias para liderar projetos de mudança social. Além disso, Etzkowitz et al. (2020) apontam que a participação de mulheres em ecossistemas de inovação pode ter um impacto positivo nas empresas e na sociedade em geral. Segundo os

autores, além de promover igualdade e justiça social, a diversidade de gênero também pode aumentar a criatividade e a inovação.

Diante disso, é importante entender a relação entre o ecossistema de inovação e a mudança social das mulheres, a fim de identificar os fatores que facilitam ou dificultam a participação das mulheres nesses ecossistemas. Como Arundel et al. (2017) definem ecossistemas de inovação como agrupamentos complexos e dinâmicos de atores, recursos e instituições que interagem para criar, disseminar e usar novos conhecimentos e tecnologias. Nesse sentido, é importante avaliar como esses atores, recursos e instituições podem ser aprimorados para promover a inclusão e a diversidade de gênero, a fim de promover uma mudança social mais justa e sustentável.

## 2. Metodologia

A metodologia de pesquisa baseou-se no método hipotético-dedutivo, por meio da construção de conjecturas (MARCONI

& LAKATOS, 2017). Foi construído a partir de dados relacionados ao Ecossistema de Inovação Brasileiro, coletados pelo Google e no portal da transparência e SECTI – Secretaria de Estado de Ciência Tecnologia e Inovação de Goiás, por meio dos nos relatórios de Mapeamento Do Ecossistema Goiano de Inovação - 2022 elaborado em conjunto pelas equipes da Secretaria de Estado de Desenvolvimento e Inovação – SEDI, Serviço de Apoio às Micro e Pequenas Empresas de Goiás - SEBRAE GO e Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO).

A metodologia de análise de dados com base em relatórios de mapeamento do ecossistema de inovação é um processo fundamental para a compreensão e a promoção da inclusão de mulheres nos espaços de Inovação e Empreendedorismo. Essa metodologia consiste em um conjunto de técnicas e ferramentas para coletar, processar, analisar e interpretar dados relevantes sobre o ecossistema de inovação local.

### QUADRO 2 – DOCUMENTO INSTITUCIONAIS

Item	Documento	Ano	Instituição
1	Ecossistema de Inovação - Região de Anápolis, Goiânia e Região Metropolitana, Setores Prioritários para o desenvolvimento da região	2019	SEBRAE GO / ANPROTEC
2	Mapeamento do Ecossistema Goiano de Inovação	2022	SEDI /SEBRAE GO/ UNESCO
3	Guia do Marco Legal de Inovação do Estado de Goiás	2023	SEDI / UNESCO

Fonte: Elaboração própria

### 3. Resultados Alcançados

Os resultados do estudo são necessários para confirmar as hipóteses e objetivos propostos. Segundo Flick (2019), “os resultados são o cerne da pesquisa empírica porque representam o que a pesquisa encontrou e alcançou” (p. 200). Portanto, a análise e interpretação dos resultados devem ser criteriosas e embasadas teoricamente para se obter conclusões confiáveis e sólidas.

Com base na revisão da literatura e análise de dados, os resultados alcançados nas comunidades empreendedoras e inovadoras de mulheres podem ser resumidos da seguinte forma:

- As comunidades empreendedoras e inovadoras de mulheres provaram ser fatores-chave na criação de um ambiente mais inclusivo e igualitário para o desenvolvimento do empreendedorismo feminino. - Essas comunidades foram capazes de fornecer às mulheres empreendedoras apoio, mentoria, networking e acesso a recursos que aumentaram sua participação no mercado de trabalho e empreendedorismo.

-As comunidades de empreendedorismo e inovação de mulheres também têm desempenhado um papel importante na promoção da diversidade e inclusão no ecossistema de inovação, o que pode levar a soluções mais criativas e eficazes para os desafios sociais.

- Além disso, essas comunidades

foram capazes de construir uma rede de mulheres empresárias e inovadoras em todo o país e criar um ecossistema de apoio e colaboração que pode promover ainda mais o crescimento do empreendedorismo feminino e da inovação liderada por mulheres.

No entanto, é importante ressaltar que ainda há desafios a serem superados para garantir a igualdade de oportunidades para as mulheres empreendedoras e inovadoras no Brasil. Estas comunidades devem continuar a ser apoiadas e fortalecidas para que possam continuar a desempenhar um papel fundamental na construção de um ecossistema de inovação mais inclusivo e diversificado.

O mapeamento destacou 12 principais comunidades brasileiras voltadas para Inovação e Empreendedorismo, a maioria delas se concentram em Goiás e São Paulo, conforme GRÁFICO 1 a seguir.

GRÁFICO 1 - % COMUNIDADES DE MULHERES POR ESTADO



O mapeamento identificou 12 principais comunidades brasileiras voltadas para inovação e empreendedorismo feminino, a maioria delas concentradas em Goiás e São Paulo. Esse resultado reforça a importância dessas regiões como centros de inovação e empreendedorismo feminino no país. A GRÁFICO 1 pode fornecer uma visualização mais clara dos resultados encontrados no mapeamento, possibilitando uma análise mais profunda das comunidades detectadas e a distribuição geográfica dessas comunidades. Além disso, esse resultado pode ser utilizado para orientar políticas públicas voltadas ao incentivo ao empreendedorismo feminino em áreas onde as comunidades ainda não estão estabelecidas.

#### **4. Considerações Finais**

A participação das mulheres nos ecossistemas de inovação e governança é fundamental para alcançar a igualdade de gênero e promover o desenvolvimento sustentável. O objetivo deste artigo foi analisar a conexão entre o ecossistema de inovação e as mudanças sociais das mulheres e descobrir os fatores que promovem ou dificultam a participação das mulheres no ecossistema de inovação.

Os resultados mostram que, embora os ecossistemas de inovação sejam importantes para o desenvolvimento do empreendedorismo e da inovação liderada por mulheres, as mulheres ainda

enfrentam desafios significativos para participar de ecossistemas de inovação e empreendedorismo. A falta de diversidade nos ecossistemas de inovação pode limitar a criatividade e a inovação, tornando a participação das mulheres fundamental para promover a diversidade e a inovação. Acesso a capital, mentoria e redes de apoio são essenciais para o sucesso de projetos de mudança social liderados por mulheres, e iniciativas que apoiem o empreendedorismo feminino e promovam a inclusão de mulheres em ecossistemas de inovação devem ser promovidas.

Nesse sentido, políticas e estratégias devem ser desenvolvidas para promover a igualdade de gênero e a justiça social com o objetivo de incluir as mulheres nos ecossistemas de inovação e empreendedorismo. A diversidade e a participação das mulheres nos ecossistemas de inovação são importantes não apenas para promover a igualdade de gênero, mas também para benefícios econômicos e desenvolvimento sustentável. Portanto, é necessário continuar pesquisando e promovendo iniciativas que promovam a participação de mulheres em ecossistemas de inovação e gestão.

## Bibliografia

ALMEIDA, R. V. de et al. Ecosistema de Inovação e Empreendedorismo de Goiás: mapeamento e análise. Goiânia: Sebrae Goiás, 2017.

ARUNDEL, A.; FUGLIE, K.; KABLA, I.; NARROG, B. The changing landscape of science and technology indicators: challenges and policy implications. *Science and Public Policy*, v. 44, n. 3, p. 287-299, 2017.

BANCO MUNDIAL. Women, Business and the Law 2019: A Decade of Reform. Washington, DC: World Bank Group, 2019.

BARLACH, Lisete. A criatividade humana sob a ótica do empreendedorismo inovador. 2009. Tese de Doutorado. Universidade de São Paulo.

CASTELLS, Manuel. A sociedade em rede. Tradução: Roneide Venancio Majer. 6ª Ed. São Paulo: Paz e terra, 1999.

ETZKOWITZ, H.; WEBSTER, A.; HELEYSSEN, B. V.; LOPEZ-VARELA, A.; MILÁN-GARCÍA, Ó.; RABELLOTTI, R.; ROSA, J. M.; SCOTT, S. Women in the entrepreneurial university: faculty, policy and practice - introduction. In: ETZKOWITZ, H.; WEBSTER, A.; HELEYSSEN, B. V. (eds.). Women in the entrepreneurial university: faculty, policy and practice. Cheltenham: Edward Elgar Publishing, 2020. p. 1-26.

FARAH, Marta Ferreira Santos. Gênero e políticas públicas. *Revista Estudos Feministas*, v. 12, n. 1, p. 47-71, 2004.

FLICK, Uwe. Introdução à pesquisa qualitativa. Porto Alegre: Artmed, 2019.

FREIRE, F.; GUERRA, S. S. Ecosistemas de Inovação: um panorama das principais definições, conceitos e modelos. IN: Encontro Nacional de Engenharia de Produção, 40, 2020, Gramado. Anais eletrônicos... Gramado, RS: ABEPRO, 2020.

GALBRAITH, C.; VICKERS, J. Women's Entrepreneurship and Economic Empowerment. London, UK: ODI, 2019.

GASCOIGNE, Adriana. Girls in Tech: Empowering Women in Technology. 2019. Disponível em: <https://www.girlsintech.org/>. Acesso em: 10 abr. 2023.

GIL, A. C. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2017.

GUPTA, Alok; KRISHNAN, Hari. Building Inclusive Innovation Ecosystems: The Role of Women Entrepreneurs. *Journal of Technology Management & Innovation*, v. 16, n. 1, p. 22-30, 2021.

La Rovere, R.L., de Oliveira Santos, G. and Vasconcellos, B.L.X., 2021. Desafios para a mensuração de Ecosystemas de Inovação e de Ecosystemas de Empreendedorismo no Brasil. *Revista de Empreendedorismo e Gestão de Pequenas Empresas*, 10(1), p.6.

LERNER, Miriam; ALMEIDA, André. The Importance of Women's Entrepreneurship Communities in the Brazilian Innovation Ecosystem. In: SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI), 33rd, 2020, Virtual. *Proceedings...* Los Alamitos, CA, USA: IEEE Computer Society, 2020. p. 446-452.

MAHAJAN, A.; LUNDBERG, E. Diversity and innovation: a practical guide to promoting inclusivity in R&D ecosystems. Boston Consulting Group, 2019.

ONU Mulheres. (2021). Igualdade de gênero e desenvolvimento sustentável. Disponível em: <https://www.unwomen.org/pt/what-we-do/sustainable-development>

SANTOS, T. C.; NASCIMENTO, L.; ARAÚJO, C. A.; COSTA, T. J. L.; SOUSA, M. A. B.; SOUZA, A. C. A.; SILVA, R. B. A mulher na liderança empreendedora no Nordeste brasileiro: um estudo a partir das experiências de mulheres empreendedoras de Teresina/PI. In: CONGRESSO INTERNACIONAL DE GÊNERO E DIVERSIDADE, 5., 2021, Natal. *Anais eletrônicos...* Natal: UFRN, 2021.

SILVA, Larisse Fernanda Ribeiro da. Mulheres no ambiente de inovação: uma investigação sobre a atuação de mulheres em startups apoiadas pelo programa Inova Maranhão no ciclo 2019/2020. 2020.

Steinem, G. (2016). *O futuro é feminino*. Editora Best Seller.

WELTER, F.; AL-LAHAM, A.; AROCHA, J.; CHEN, W.; DE LA CRUZ, A.; ELIAS, S.; ETZKOWITZ, H.; GALAN-MARTIN, A.; KUMAR, A.; LOPEZ-FERNANDEZ, M. C.; et al. Women's entrepreneurship in the Middle East and North Africa (MENA) region: opportunities and challenges. *Gender in Management: An International Journal*, v. 33, n. 2, p. 122-139, 2018.

# EDUCAÇÃO EMPREENDEDORA E SEUS IMPACTOS NO CRESCIMENTO DO EMPREENDEDORISMO DE OPORTUNIDADE

## RESUMO

A Educação Empreendedora tem sido amplamente discutida no contexto brasileiro, principalmente em relação aos seus impactos no crescimento do empreendedorismo de oportunidade. Dessa forma, o objetivo geral do artigo consiste em descrever os reais impactos da Educação Empreendedora nesse tipo de empreendedorismo. Para alcançar esse objetivo elencou-se os objetivos específicos: apresentar o crescimento significativo dos microempreendedores, demonstrar os impactos de crescimento do empreendedorismo de oportunidade, estudar os efeitos da atividade empreendedora sobre o crescimento econômico e o desemprego no Brasil, e apresentar metodologias de ensino empreendedor. Esta revisão bibliográfica utilizou-se base de dados eletrônicas, artigos científicos, revistas, dados do SEBRAE e outras fontes relevantes para o tema, visando uma análise abrangente e atualizada. Visando contribuir para a compreensão dos benefícios e desafios da Educação Empreendedora e para o desenvolvimento de novas estratégias de incentivo ao empreendedorismo, o que pode ser útil para gestores públicos e educadores que buscam estimular o empreendedorismo e o desenvolvimento econômico em suas regiões. Os resultados mostram que o empreendedorismo de oportunidade

representa uma alternativa valiosa no combate ao desemprego e incentivo ao desenvolvimento econômico. O ensino do empreendedorismo envolve mudança de pensamentos e exige muito foco no aprendizado. A Educação Empreendedora (EE) pode capacitar pessoas para identificar e criar oportunidades por meio da inovação. Portanto, conclui-se que a Educação Empreendedora representa uma importante ferramenta para estimular o empreendedorismo de oportunidade no Brasil, contribuindo para o crescimento econômico e a redução do desemprego no país.

**Palavras chave:** Conhecimento. Característica e habilidade. Pensamento criativo. Atividade empreendedora. Metodologias de ensino.

## 1. INTRODUÇÃO

Recentemente, permanecem diversas definições e teorias acerca do termo “empreendedorismo”, que dão dois fluxos distintos: a primeira de economistas que acoplam empreendedorismo a novidades (CHAGAS, 2006), e a secundária teoria contemporânea, ressaltando aspectos atitudinais de ser empreendedor, como a capacidade criadora por oportunidade.

A expressão empreendedorismo surgiu por volta do século XVII (HISRICH; PETER, 2004) e foi vigorosamente

propagada pelo economista Richard Cantillon. Em um artigo, se revelou um buscador de oportunidades de negócios, preocupado em fazer uma gestão inteligente auferir e otimizar receitas. Já o economista, Jean-Baptiste Say, defendia que o desenvolvimento econômico era resultado da criação de novos negócios era consequência da fundação de novas empresas, junto a expansão da Revolução Industrial. Para Cantillon e Say, um empreendedor é alguém que assume riscos, basicamente porque coloca seu próprio dinheiro, assume os riscos inerentes ao aproveitar as oportunidades com vistas ao lucro. A dupla não estava interessada apenas em economia, mas também em criar novos negócios. (BAGGIO; BAGGIO, 2014).

William Baumol e Joseph Schumpeter, também forneceram teorias para ampliar a compreensão do termo. Eles vinculam explicitamente o empreendedorismo à inovação, apontam que o start do empreendedorismo está em entender e cultivar novas oportunidades no campo dos negócios e definem os empreendedores como agentes centrais no processo de mudança socioeconômica (BAGGIO; BAGGIO, 2014).

No Brasil, o tema progrediu e ganhou mais espaço e coesão. Além das instituições de ensino superior, o assunto também diz respeito às escolas formais, incluindo programas de apoio ao ensino. Em meados da década de 1990, o professor Fernando Dolabela, considerado fundador do empreendedorismo no Brasil,

adolesceu a teoria do empreendedorismo como contorno de inclusão social, que apodou de “teoria dos sonhos” (BAGGIO; BAGGIO, 2014).

Para que possa se compreender os objetivos deste estudo, serão utilizados dados do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE) e Serasa Experian, que de acordo com a primeira instituição, a adjacência empreendedorismo se faz com a habilidade para resolver dificuldades, acender oportunidades, inventar soluções e focar na educação de ideias ressaltantes a seu público e a sociedade. O empreendedorismo permanece com força no Brasil e ganha popularidade atrelada a uma estratégia para encarar os efeitos desumanos do desemprego crescente (SEBRAE, 2021).

A problemática desse artigo incide em como a Educação Empreendedora pode alavancar o crescimento de empreendedores, e descobrir qual são os impactos causados no Brasil com tal crescimento, atrelado a Educação Empreendedora. Visto que é preciso expor o empreendedorismo como uma atividade que influencia o desenvolvimento econômico e social e expor o seu impacto a nível nacional. Enfatizando a importância de compreender os benefícios e desafios da Educação Empreendedora e a elaboração de novas estratégias de incentivo ao empreendedorismo.

Portanto, neste trabalho foi realizado pesquisas bibliográficas exploratórias e descritivas que serão conduzidas

utilizando métodos de dados qualitativos derivados de fundamentos científicos como Google acadêmico e SEBRAE e Serasa Experian. Também pesquisas sobre o tema serão baseadas em artigos científicos acadêmicos online e impressos e nos principais sites brasileiros relacionados a empreendedorismo e negócios. Especialmente no que se refere à Educação Empreendedora.

O objetivo geral consistiu em descrever os reais impactos da Educação Empreendedora no empreendedorismo por oportunidade. Seus objetivos específicos são: 1) apresentar o crescimento significativo dos microempreendedores; 2) demonstrar os impactos de crescimento do empreendedorismo de oportunidade; 3) procura-se examinar o efeito da atividade empreendedora sobre o crescimento econômico e o desemprego, analisando o Brasil e 4) apresentar metodologias de ensino empreendedor.

## 2.DEMANDAS POR CARACTERÍSTICAS EMPREENDEDORAS

O alvo central deste estudo é demonstrar que a Educação Empreendedora necessita ser desigual do típico ensino em negócios, a Educação Empreendedora carece focalizar em lideranças, desenvolvimento de novos serviços e produtos, negociações, apresentação ao que é novo, e no que diz respeito a empreendedorismo de oportunidade, o pensamento criativo, e outros pontos correlatos (MARTENS; FREITAS, 2008). Outra propriedade, incorporada à Educação Empreendedora é de ser uma ação comunicativa, onde através de diversas metodologias dialogadas, os interessados se desenvolverão (TSCHÁ; CRUZ NETO, 2014).

Sebrae (2021), enfatiza que a base sólida de conhecimento acerca do empreendedorismo, faz com que através da interação social, as seguintes quatro características ligadas a experiência empreendedora se desenvolva.

Quadro 01- Características de um empreendedor:

<b>Autoconfiança:</b>	Confiar no seu potencial é fundamenta para os que querem seguir o empreendedorismo
<b>Coragem:</b>	O receio do frustrar-se não deve ser superior que o anseio de se tornar bem-sucedido. Essa é característica que adolece a percepção acerca da possibilidade de falha.
<b>Persistência:</b>	Se manter sempre firme diante das dificuldades, procurando sempre soluções para passar por obstáculos que poderão surgir, manter motivado continuamente
<b>Otimismo:</b>	Ininterruptamente confiar o mais perfeito de si, confiando que no fim tudo dará certo, para alcançar os objetivos é fundamental

Com as características de competências e, assim, não há empreendedoras atreladas a aprendizagem empreendedora faz-se com que o processo de desenvolvimento para começar novos negócios se torne um processo contínuo, no qual facilita ainda mais na metodologia da Educação Empreendedora, sendo as noções ocorridos da experiência particular do empreendedor e aproveitados para conduzir a opção de novas experiências (POLITIS, 2005). Esta metodologia “representa o meio pelo qual se adquire a competência, enquanto a competência representa a manifestação do que o indivíduo aprendeu” (DE FREITAS; BRANDÃO, 2009, p. 100).

Afim de haver o desenvolvimento da aprendizagem empreendedora se faz necessário reforçar as competências pessoais, sendo a aprendizagem e a competências acometidos que se fazem complementares. Sendo que, o aumento das competências se repousa em um artifício contínuo de aprendizagem, criando assim uma rotina de melhorias (BITENCOURT, 2005). Em suma, a aprendizagem é um processo imprescindível para o alcance

de desenvolvimento sem aprendizagem.

### 3. NASCIMENTO DE EMPRESAS NO BRASIL X EDUCAÇÃO EMPREENDEDORA

Em levantamentos realizadas pelo Serasa Experian (2023), somente no mês de janeiro de 2021 foram abertos mais de 312 mil novos registros de microempreendedores individuais, um recorde até novembro de 2022 no Brasil, o maior da série desde 2018, como registrado pelo gráfico 01, demonstra crescimento significativo do perfil empreendedor, mais profundamente falando como mostra o gráfico, o ano de 2021 foi o que mais houve nascimento de micro empreendedores, observando que o ano de 2022 ainda não foi totalmente contabilizado, porem seguindo tendencias de crescimento é provável fortemente que ultrapasse o ano de 2021.

Gráfico 01- Quantidade de MEI X Nascimento de empresas no Brasil nos últimos cinco anos



# INTERNET DAS COISAS VERSUS LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: UM CONFRONTO EM PROL DA SEGURANÇA E DOS DIREITOS FUNDAMENTAIS.

## RESUMO

O presente estudo tem como principal foco abordar a Internet das Coisas (IoT) e a Lei Geral de Proteção de dados (LGPD), relacionadas à segurança e aos direitos fundamentais. O objetivo geral é identificar os principais riscos da IoT à segurança e aos direitos fundamentais, verificando o papel da LGPD, dentre outras normas, na qualidade de instrumentos a fim de amenizar tais riscos. Para tanto, definiram-se os seguintes objetivos específicos, conceituar a IoT. Compreender os objetivos da LGPD e seus princípios norteadores. Identificar os riscos que a IoT apresenta aos usuários. E compreender a importância dos direitos fundamentais aliados à LGPD, para garantir a segurança e a privacidade dos dados pessoais. Discutir sobre a Internet das Coisas (IoT) e a Lei Geral de Proteção de Dados Pessoais (LGPD), justifica-se pela quantidade astronômica de dados coletados pelos dispositivos da IoT, os quais são tratados, armazenados e eventualmente compartilhados ou até mesmo comercializados. Diante disso, é possível notar os riscos envolvendo a segurança desses dados. O presente estudo consiste em uma pesquisa aplicada, de caráter exploratório. Utilizou-se o método descritivo, envolvendo, sobretudo, pesquisas realizadas a partir

de levantamentos bibliográficos. Verifica-se que o armazenamento seguro de dados pessoais em dispositivos da IoT é um desafio complexo, que requer conformidade com as normas legais, em especial com a LGPD. Os conteúdos aqui apresentados demonstram que muitas outras pesquisas ainda podem ser realizadas sobre o tema, devido sua importância para o meio acadêmico, jurídico e toda a sociedade.

**Palavras chave:** Internet das coisas. LGPD. Dados pessoais. Segurança. Privacidade.

## ABSTRACT

The main focus of this study is to address the Internet of Things (IoT) and the General Data Protection Law (LGPD), related to security and fundamental rights. The general objective is to identify the main risks of IoT to security and fundamental rights, verifying the role of the LGPD, among other standards, as instruments to mitigate such risks. To this end, the following specific objectives were defined, to conceptualize the IoT. Understand the objectives of the LGPD and its guiding principles. Identify the risks that IoT presents to users. And understand the importance of fundamental rights allied to the LGPD, to ensure the security and privacy of personal data.

Discussing the Internet of Things (IoT) and the General Law for the Protection of Personal Data (LGPD) is justified by the astronomical amount of data collected by IoT devices, which are processed, stored and eventually shared or even commercialized. Given this, it is possible to notice the risks involving the security of this data. The present study consists of an applied research of an exploratory nature. The descriptive method was used, involving, above all, research carried out from bibliographic surveys. It appears that the secure storage of personal data on IoT devices is a complex challenge, which requires compliance with legal standards, in particular with the LGPD. The contents presented here demonstrate that many other researches can still be carried out on the subject, due to its importance for the academic, legal and society as a whole.

**Key words:** Internet of things. LGPD. Personal data. Security. Privacy.

## 1. INTRODUÇÃO

O presente artigo tem como foco principal abordar a Internet das Coisas (IoT) e a Lei Geral de Proteção de dados (LGPD), relacionadas à segurança e aos direitos fundamentais do usuário, isto é, da pessoa natural.

De acordo com Burkart (2021), é imperioso que as pessoas tenham conhecimento dos seus direitos. Contudo,

ainda existe uma lacuna entre a legislação e o saber, o que significa que mesmo que haja leis que tratem do assunto, os indivíduos não estão totalmente protegidos se não tiverem conhecimento dos seus direitos. Por isso, deve haver esforços para tornar o conhecimento jurídico mais acessível e compreensível para o público em geral.

Sendo assim, discutir sobre a Internet das Coisas (IoT) e a Lei Geral de Proteção de Dados Pessoais (LGPD), justifica-se pela quantidade astronômica de dados coletados pelos dispositivos da IoT, os quais são tratados, armazenados e eventualmente compartilhados com instituições parceiras, ou até mesmo comercializados com terceiros.

Diante disso, é possível notar os riscos envolvendo a segurança desses dados. E a falha da segurança pode ocasionar exposição de dados pessoais sensíveis, o que atingiria diretamente os direitos fundamentais do usuário titular. Dentre esses direitos, destacam-se a privacidade, a liberdade e o livre desenvolvimento da personalidade da pessoa natural.

Ademais, conceituar a IoT e compreender os objetivos da LGPD torna-se imprescindível para identificar os riscos que os dispositivos conectados (IoT) apresentam aos usuários. Nesse sentido, revela-se crucial o conhecimento da aliança formada entre os direitos fundamentais e a LGPD, como instrumentos garantidores da segurança e da privacidade dos dados

peçoais dos usuáios.

Portanto, o presente artigo estabeleceu como problema de pesquisa: Quais os principais impactos da Internet das Coisas sobre a Segurança e os Direitos Fundamentais? A Lei Geral de Proteção de Dados Pessoais é um instrumento eficiente para amenizar esses impactos? Tendo como objetivo geral, identificar os principais riscos da Internet das Coisas à segurança e aos Direitos Fundamentais de seus usuáios, verificando o papel da LGPD dentre outras normas, na qualidade de instrumentos eficazes para combater tais riscos.

Para alcançar o objetivo geral, os objetivos específicos serão conceituar a IoT (Internet das Coisas). Compreender os objetivos da LGPD (Lei Geral de Proteção de Dados Pessoais) e seus princípios norteadores. Identificar os riscos que a IoT apresenta aos seus usuáios. E, compreender a importância dos direitos fundamentais aliados à LGPD, como medidas para garantir a segurança e a privacidade dos dados pessoais dos usuáios da IoT.

## 2. METODOLOGIA

O presente estudo consiste em uma pesquisa aplicada, de caráter exploratório, que segundo Gil (2002, p.41): “(...) tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito. Pode envolver levantamento

bibliográfico ou entrevistas com pessoas experientes no problema pesquisado.”

Sendo assim, esta pesquisa tem como finalidade identificar os principais riscos da Internet das Coisas à segurança e aos Direitos Fundamentais de seus usuáios, verificando o papel da Lei Geral de Proteção de Dados Pessoais dentre outras normas, na qualidade de instrumentos eficazes para amenizar tais riscos.

Esta pesquisa também utilizou do método descritivo, visando analisar, observar, registrar e correlacionar aspectos encontrados em entendimentos legais e doutrinários. Envolvendo, sobretudo, pesquisas realizadas a partir de levantamentos bibliográficos.

Nesse sentido, como fontes de pesquisa, a fim de desenvolver o referencial teórico da presente revisão de literatura, foram utilizados livros, artigos e sites contendo legislações atualizadas, todos relacionados ao tema.

## 3. INTERNET DAS COISAS (IOT)

A Internet das Coisas (IoT) apresenta-se como uma das tecnologias mais importantes do século XXI, sendo caracterizada por uma rede de objetos, dispositivos, dentre outras tecnologias que estão se comunicando, isto é, colhendo e repassando dados (ORACLE, 2021).

No que tange a origem do termo IoT “Internet of Things”, acredita-se que foi

empregado por Kevin Ashton, o qual desde o ano de 1999 destaca a necessidade das pessoas se conectarem à internet, em virtude da limitação de tempo imposta pela rotina (ASTHON, 2009).

De acordo com Santos et. al., (2017, p. 2) “a conexão com a rede mundial de computadores viabiliza primeiro, controlar remotamente os objetos e, segundo, permitir que os próprios objetos sejam acessados como provedores de serviços”. Quanto aos objetos controlados pela IoT, tem-se uma variedade de dispositivos cotidianos, além de computadores e celulares, verificam-se relógios, televisões, geladeiras, carros etc.

Ademais, conforme a IoT evolui,

concretiza-se a ideia de conectar o mundo, resultando em uma grande quantidade de dados sendo coletados por seus dispositivos, em tempo real. Diante disso, estima-se que até o ano de 2025 haja cerca de 73,1 bilhões de zettabytes armazenados por essa tecnologia (IDC, 2020).

Sob o viés jurídico, verifica-se a conceituação de IoT no Decreto nº. 9.854/2019 (Plano Nacional de Internet das Coisas). E visando facilitar a compreensão do leitor, o legislador trouxe também, individualmente, o conceito de coisas, dispositivos e serviços de valor adicionado. Vejamos os referidos conceitos na tabela adiante.

**Internet das Coisas (IoT):** 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.

<b>Coisas:</b> objetos no mundo físico ou no mundo digital, capazes de serem identificados e integrados pelas redes de comunicação.	<b>Dispositivos:</b> equipamentos ou subconjuntos de equipamentos com capacidade mandatória de comunicação e capacidade opcional de sensoriamento, de atuação, de coleta, de armazenamento e de processamento de dados.	<b>Serviço de valor adicionado:</b> atividade que acrescenta a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações, nos termos do disposto no art. 61 da Lei nº 9.472, de 16 de julho de 1997.
---	---	---

**FONTE:** Artigo 2º, incisos I a IV, do Decreto nº. 9.854/2019 (Plano Nacional de Internet das Coisas)

Compreende-se, em suma, que a IoT se trata de uma infraestrutura (tecnologia), integrada a objetos físicos ou digitais, os quais são conectados à dispositivos com capacidade de comunicação, coleta, armazenamento e processamento de dados (BRASIL, 2019).

Segundo (SANTOS et al., 2017), o modelo de arquitetura (infraestrutura) básica da IoT possui três camadas. Percepção. Rede. Aplicação. A Percepção está representada por objetos físicos ou digitais, dispositivos eletrônicos e sensores aplicados nos ambientes, a fim de coletar dados, respondendo de acordo com o proposto. A rede contempla as abstrações das tecnologias de comunicação, serviços de gerenciamento, roteamento e identificação. Por fim, a camada de aplicação é responsável por dispor os serviços aos usuários.

Atualmente, é possível deparar-se com ambientes automatizados, os quais são controlados por smartphones e tablets. Estima-se que com os avanços da tecnologia, não serão necessários o uso destes dispositivos para controlar o ambiente. Contudo, para que os ambientes possam reagir à presença dos usuários, controlando-se sozinhos, será preciso de uma grande quantidade de sensores espalhados no local, o que possivelmente acarretará em mais riscos para a segurança de informações, bem assim, a privacidade (FIGUEIRA, 2016).

#### **4. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

As discussões envolvendo políticas de privacidade, uso, processamento e segurança de dados pessoais não são recentes. Muito embora o Marco Civil da Internet (Lei nº. 12.965/2014) tenha estabelecido direitos, garantias e deveres para utilização da internet no Brasil, ainda se vislumbrava necessário aprofundar as normas, adaptando-as à crescente evolução tecnológica.

Diante disso, em 14 de agosto de 2018 foi publicada a Lei Geral de Proteção de Dados Pessoais (LGPD), dispendo “sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018).

A LGPD (Lei nº. 13.709/2018) objetiva proteger os direitos de liberdade e privacidade das pessoas. Por conseguinte, para promover a proteção dos dados pessoais dos cidadãos brasileiros, criou-se um cenário de segurança jurídica, norteado por parâmetros internacionais efetivos, mediante a regulamentação e padronização das práticas dos usuários.

Porém, a LGPD sofreu diversas prorrogações, e somente no mês de setembro do ano de 2020 sua redação

entrou em vigor. A partir da vigência, houve a obrigatoriedade das organizações se adaptarem às suas práticas, sob pena de sanções administrativas, dentre elas, multas exorbitantes, a fim de enfatizar para as empresas e os usuários, a importância de seguir as diretrizes regulamentadas.

O art. 5º, I, da LGPD dispõe que dado pessoal trata-se de “informação relacionada a pessoa natural identificada ou identificável”. Posteriormente, no art. 7º da lei, verifica-se, taxativamente, as hipóteses em que os dados pessoais poderão ser tratados. A primeira delas é mediante o consentimento do usuário titular à política de privacidade.

A referida política exige a obrigação de transparência, isto é, de informar ao usuário sobre tudo relativo ao tratamento de seus dados. Por exemplo, quanto tempo os dados ficarão armazenados, a forma como serão coletados, a finalidade, se os dados serão compartilhados, ou comercializados com terceiros. E tal obrigatoriedade atinge todas as pessoas jurídicas de direito público e privado que de alguma forma coletam dados no país. (BRASIL, 2018)

A LGPD disciplina medidas técnicas e administrativas, visando proteger os dados pessoais e sigilosos dos usuários, contra acessos não autorizados. E medidas de segurança quanto a situações ilícitas de destruição, ou acidentais, alteração, perda, comunicação, ou difusão dos dados. Contudo, embora a lei ofereça orientações básicas para a regulamentação de serviços,

acredita-se que será desafiador encontrar um ponto de equilíbrio entre o tratamento dos dados e o os direitos de privacidade dos usuários. (NOBRE et al., 2019).

Logo, as empresas, sobretudo, devem adequar-se às normas, oferecendo um ambiente seguro para os dados coletados, a fim de reduzir os riscos de ataques cibernéticos. Pois, se houver vazamento de dados, mesmo que sejam decorrentes de hackers e malwares, o fato deverá ser comunicado aos usuários e à Autoridade Nacional de Proteção de Dados (ANPD), bem assim, a empresa será responsabilizada, inclusive deverá tomar providências que amenizem eventuais impactos causados, diante da quebra de privacidade.

Importante conceito abordado pela LGPD trata-se do dado pessoal sensível, previsto expressamente como o dado pessoal que mantém informações “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” (artigo 5º, II, da LGPD).

Os dados pessoais sensíveis integram o núcleo da privacidade do usuário titular. Ademais, considerando que seu conteúdo é passível de discriminação, por revelar a cor da pele, orientação sexual, política, religiosa, alguma doença etc., apresentam riscos aos direitos e liberdades

fundamentais do usuário. Diante disso, são tutelados com maior rigidez. (TEPEDINO, 2019, p. 307)

No que tange ANDP, trata-se de uma autarquia de natureza especial, responsável por “fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso”, dentre outras atribuições relacionadas à LGPD (BRASIL, 2018).

Conclui-se, portanto, que o armazenamento dos dados é visto como um trabalho complexo na IoT, diante da dificuldade em realizar alterações

físicas nos dispositivos, para adequá-los à LGPD. Uma alternativa para chegar a uma solução está no uso de criptografia, no armazenamento dos dados, o que aumentaria sua segurança. (NOBRE et al., 2019, p. 11)

#### 4.1 Princípios relativos ao Tratamento dos Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD) apresenta em seu art. 6º, incisos I a X, um rol de princípios necessários às atividades de tratamento de dados pessoais, dispondo ainda que tais atividades deverão observar a boa-fé dos usuários.

Vejamos os princípios:

FINALIDADE	ADEQUAÇÃO
NECESSIDADE	LIVRE ACESSO
QUALIDADE DOS DADOS	TRANSPARÊNCIA
SEGURANÇA	PREVENÇÃO
NÃO DISCRIMINAÇÃO	RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Cada inciso do art. 6º traz uma breve explicação, para o respectivo princípio.

O princípio da finalidade refere-se à realização do tratamento dos dados, para propósitos legítimos, que sejam ainda, específicos e explícitos, devendo ser informados ao usuário titular. Excluindo a possibilidade de tratamento posterior que seja incompatível com as finalidades. (BRASIL, 2018)

Verifica-se em seguida, os princípios da adequação e da necessidade. Visto que se faz necessário haver compatibilidade do tratamento dos dados, com as finalidades informadas ao usuário e o contexto do referido tratamento. Defende-se então, a limitação do tratamento dos dados coletados ao mínimo necessário, para a realização de suas finalidades, abrangendo dados pertinentes, de modo proporcional e não excessivo. (BRASIL, 2018)

Quanto ao princípio do livre acesso, dispõe sobre a garantia dos usuários titulares, de realizarem consulta gratuita e facilitada a respeito da forma e duração do tratamento de seus dados pessoais, bem assim, no que diz respeito à integralidade desses dados. (BRASIL, 2018)

Nesse sentido, o princípio da qualidade dos dados, visa garantir aos usuários titulares, clareza, exatidão, relevância e atualização de seus dados, conforme a necessidade e o cumprimento da finalidade do tratamento. (BRASIL, 2018)

No que se refere ao princípio da transparência, trata dos direitos garantidos

aos usuários titulares, de obterem informações claras, precisas e de fácil acesso, quanto à realização do tratamento de seus dados pessoais, bem assim, sobre os respectivos agentes responsáveis pelo tratamento, excetuados, contudo, segredos comerciais e industriais. (BRASIL, 2018)

O princípio da segurança, refere-se à utilização de medidas técnicas e administrativas competentes para proteger os dados pessoais dos usuários de acessos não autorizados, decorrentes de situações ilícitas de destruição, ou acidentais, alteração, perda, comunicação, ou difusão dos dados pessoais. (BRASIL, 2018)

Em consonância com a segurança, tem-se o princípio da prevenção, no qual se busca adotar medidas, visando prevenir ocorrência de danos, em razão do tratamento de dados. (BRASIL, 2018)

Destaca-se em seguida, o princípio da não discriminação, referindo-se à impossibilidade de realizar o tratamento de dados pessoais, para fins discriminatórios, abusivos e ilícitos.

E disposto no inciso X, verifica-se o princípio da responsabilização e prestação de contas dos responsáveis pelo tratamento dos dados. Esse princípio tem como objetivo demonstrar a adoção de medidas efetivas, buscando o cumprimento das normas de proteção de dados pessoais e a eficácia de seus dispositivos. (BRASIL, 2018)

Percebe-se que a observância aos princípios expressos na LGPD, torna-se essencial para diminuir, quiçá combater os danos causados aos usuários titulares de dispositivos da IoT. Ademais, trata-se de um rol de princípios exemplificativo, isto é, podem ser aplicados demais princípios e normas do ordenamento jurídico brasileiro ao caso concreto.

## 5. SEGURANÇA

Com a crescente expansão da IoT, a segurança da informação vem se tornando cada vez mais crítica, uma vez que cada dispositivo conectado pode representar um ponto de vulnerabilidade. Ainda porque tais dispositivos podem ser comprometidos por meio de códigos maliciosos, que podem ser inseridos para afetar a integridade e a segurança dos sistemas. (FIGUEIRA, 2016)

Ademais, com a popularização da Internet e a alta dos crimes cibernéticos, gerou-se grande preocupação com a segurança das informações, levando os governos a criarem normas e padrões, para orientar e organizar a implementação da segurança, com o objetivo de proteger os dados sensíveis e garantir a continuidade dos negócios. (OLIVEIRA et al., 2016)

A Segurança da Informação (SI) tem como objetivo principal proteger um conjunto de informações que possuem valor para uma pessoa ou organização, garantindo sua confidencialidade,

integridade e disponibilidade, além de resguardar a privacidade e prevenir o uso indevido ou ilícito dessas informações. (NOBRE et al., 2019).

Outrossim, para (OLIVEIRA et al., 2016, p. 39) “A SI é a responsável por salvaguardar a informação. Esta deve garantir a continuidade das atividades, a integridade da informação e a disponibilidade da informação e dos serviços da organização”.

De acordo com Maymi e Harris (2010), a Segurança da Informação é composta por três pilares principais, conhecidos como “tríade CIA”, quais sejam, confidencialidade, integridade e disponibilidade (Confidentiality, Integrity and Availability). A autenticação e o não repúdio foram adicionados à tríade posteriormente, para reforçar ainda mais a segurança da informação.

Nesse sentido, (HINTZBERGEN et al., 2018) definem os referidos pilares da segurança, haja vista que os consideram fundamentais para a SI.

Em síntese, a confidencialidade consiste na restrição da informação aos autorizados, tornando-as confidenciais. A integridade equipara-se à garantia de que a informação acessada está correta (íntegra). A disponibilidade refere-se ao acesso às informações estar disponível, para os autorizados. Quanto à autenticidade ou autenticação, trata-se da segurança de uma entidade ser o que afirma ser. E ela está

intimamente ligada à confiabilidade. Por fim, o não repúdio, trata-se da habilidade de rastrear a origem de um evento ou ação, a fim de provar sua ocorrência e revelar o responsável. (HINTZBERGEN et al., 2018)

Em pesquisa de (MONTEIRO et

al., 2021) revelou-se dados preocupantes relacionados à segurança das redes brasileiras. Ao realizar uma busca no site Shodan.io verificou 382.098 dispositivos, em todo o mundo, mantendo a senha “Admin”, isto é, a senha padrão de fábrica.



<b><u>Authentication Required</u></b>	
Nome de usuário:	<u>Admin</u>
Senha:	*****
<b>Login</b> <b>Cancel</b>	

**Imagem ilustrativa**

O Brasil está entre os 5 dos países com mais usuários que não alteraram a senha padrão. Diante disso, as redes desses usuários possuem fraquezas de segurança, facilitando ataques cibernéticos. Sendo assim, a troca da senha padrão por uma senha personalizada (exclusiva) é imprescindível para a segurança das redes IoT.

A implementação de um firewall (sistema de segurança que controla o acesso à rede) trata-se de uma ação importante que pode ser feita pelo administrador da rede, para protegê-la contra ameaças externas. No entanto, é importante ressaltar que firewalls exigem alto poder de processamento e disponibilidade de energia para operar corretamente e

alcançar seu objetivo de proteção da rede. Isso pode representar um desafio para a implementação do firewall em redes IoT, visto que os recursos de processamento e energia são geralmente limitados nos dispositivos inteligentes. (MONTEIRO et al., 2021)

Compreende-se assim, que na área da Segurança da Informação deve-se considerar que os sensores e dispositivos da IoT são mais vulneráveis e suscetíveis a quebras de segurança. Isso ocorre porque muitos softwares e processos de segurança já foram criados para proteger os servidores, mas as soluções de segurança para os dispositivos conectados ainda são relativamente novas e estão evoluindo. Logo, nesse cenário, a prioridade

fundamental trata-se de encontrar soluções efetivas, para garantir a segurança dos dados dos usuários que utilizam produtos e serviços da IoT (FIGUEIRA, 2016).

## 6. DIREITOS FUNDAMENTAIS

Diante do contexto da Internet das Coisas (IoT), surgem novos desafios para o ordenamento jurídico. Considerando a intensidade dos armazenamentos, tratamentos, compartilhamentos e, inclusive, comercializações dos dados coletados, questões como ética e a privacidade dos usuários, tornam-se pautas essenciais. (MAGRANI, 2019)

A Constituição Federal (1988) defende o direito à privacidade, dispondo no art. 5º, inc. X, 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”. A carta magna resguarda também, em seu art. 5º, inc. LXXIX (advindo da EC/115 de 2022), a proteção dos dados pessoais, por meios físicos ou digitais.

Ainda no rol de direitos fundamentais, cabe destacar o habeas data (um remédio constitucional previsto no artigo 5º, inciso LXXII da CF), que objetiva verificar informações sobre a identidade do requerente, constantes de fichas ou cadastros pertencentes a um órgão público. Bem assim, o habeas data é impetrado para realização do tratamento de dados,

quando não se referir à procedimentos judiciais, administrativos ou confidenciais.

De acordo com Doneda et. al. (2019) a proteção de dados é uma garantia de caráter instrumental. Embora derive da tutela da privacidade, não se limita a ela, pois abrange todas as garantias básicas inseridas no ordenamento jurídico brasileiro.

Segundo Gilmar Mendes (2018), o direito à privacidade é crucial para a saúde mental e o desenvolvimento da personalidade livre do indivíduo. O autor expõe que ser constantemente observado dificulta a superação de desafios.

Para Arruda (2019), os Princípios de Privacidade Geralmente Aceitos (GAAP), conceituam a privacidade como: “Os direitos e obrigações de indivíduos e organizações em relação à coleta, uso, retenção, divulgação e descarte de informações pessoais”. No que tange o termo “informação pessoal” diz respeito a qualquer informação vinculada a alguém, ou que possa identificar o um indivíduo, de forma direta ou indireta. Por exemplo: nome, sobrenome, idade, endereço, características físicas, dentre outras.

Entretanto, algumas informações são caracterizadas como sensíveis (confidenciais), exigindo maior proteção e cuidado, bem assim, o consentimento do usuário para o uso e a coleta desses tipos de dados. São exemplos de dados sensíveis: localização, condições médicas,

etnia, religião, orientação sexual etc. (ARRUDA, 2019).  
(ARRUDA, 2019).

De acordo com Moraes (2019) os conceitos constitucionais de intimidade e vida privada são interligados, mas podem ser diferenciados. A intimidade se refere às relações subjetivas e de trato íntimo da pessoa, enquanto a vida privada está relacionada aos outros relacionamentos humanos, incluindo os objetivos, como trabalho e estudo.

Há também o entendimento de que os direitos de privacidade, na presente era, estão ligados à escolha do indivíduo, pois a privacidade abrange direitos de decisão “sobre onde se quer estar no espectro entre sigilo e transparência em cada situação” (ZUBOFF, 2015, p. 48)

A personalidade de uma pessoa pode ser gravemente afetada pela divulgação e uso inadequado de informações armazenadas sobre ela. “Por se constituírem em uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade” (MENDES, 2014, p. 34). Portanto, os dados, por fazerem parte da personalidade da pessoa, merecem proteção jurídica.

Ressalta-se a importância de anonimizar todos os dados secundários, ao divulgar informações pessoais ao público, para que a identidade do indivíduo não possa ser determinada, efetivando, assim, o direito fundamental à privacidade.

Verifica-se como regra geral da LGPD “o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º da LGPD). Compreende-se assim, a exigência de uma base legal que fundamente o tratamento dos dados, observando ainda seus princípios norteadores.

Os direitos fundamentais não podem ser mitigados, isto é, não podem ser restringidos em detrimento de outros igualmente dispostos no ordenamento jurídico brasileiro. Embora a garantia à segurança pública verifique-se expressa na Constituição Federal, não se trata de valor intransponível, mesmo quando em conflito com outros direitos fundamentais, por exemplo, os direitos de intimidade e vida privada. Pois, dessa forma, estaríamos diante de uma colisão entre o exercício de dois direitos fundamentais. (DIMOULIS, et. al., 2018)

## 7. CONSIDERAÇÕES FINAIS

Os conteúdos abordados ao longo do presente artigo evidenciam a importância do confronto entre a Internet das Coisas e a Lei Geral de Proteção de Dados Pessoais, no que se refere à segurança e aos

direitos fundamentais do usuário titular das informações coletadas pelos dispositivos da IoT.

Verifica-se que o armazenamento seguro de dados pessoais em dispositivos da IoT é um desafio complexo, que requer conformidade com as normas legais, em especial com a LGPD. Nesse sentido, a fim de garantir a proteção e a privacidade dos usuários titulares, o tratamento dos dados pessoais deve ser realizado de forma responsável e transparente.

Portanto, a observância dos princípios da LGPD configura-se essencial para minimizar os danos causados aos usuários de dispositivos da IoT, visto que a lei regulamenta o tratamento de dados pessoais em ambientes digitais, realizados por pessoas físicas ou jurídicas, públicas ou privadas, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos.

Os conteúdos aqui apresentados demonstram que muitas outras pesquisas ainda podem ser realizadas sobre a Internet das Coisas e a Lei Geral de Proteção dos Dados Pessoais, diante da segurança e dos direitos fundamentais dos usuários, devido à importância do tema e as inúmeras contribuições para o meio acadêmico, jurídico, bem assim para toda a sociedade.

**Geisiana Campos Souza** (Bacharel em Direito pela FAMP; Especialista em Direito Constitucional pela UNOPAR; geisi.ana@hotmail.com)

**Geana Campos Souza** (Bacharel em Direito pela FAMP; geana.campos.souza@gmail.com)@hotmail.com)

**Virgílio Norberto de Jesus Neto** (Bacharel em Direito pela UNIEURO; Especialista em Direito Penal, Processo Penal, Administrativo e Constitucional pela Araguatins/IECO; virgilionorbertoneto@gmail.com)

---

## REFERÊNCIAS

ARRUDA, Mayke Ferreira et al. Um modelo ontológico e um serviço de gerenciamento de dados de apoio à privacidade na Internet das Coisas. 2019.

ASHTON, Kevin et al. That 'internet of things' thing. RFID journal, v. 22, n. 7, p. 97-114, 2009.

BRASIL, Constituição. República federativa do Brasil. Brasília: Senado Federal, Centro Gráfico, 1988.

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. Brasília: Secretaria-Geral, 2019.

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: Casa Civil, 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Secretaria-Geral, 2018.

BURKART, D. V. V. Proteção de dados e o estudo da lgpd. Universidade Estadual Paulista (UNESP), 2021.

DONEDA, Danilo; BARRETO, Maurício Lima; DE ARAÚJO ALMEIDA, Bethânia. Uso e proteção de dados pessoais na pesquisa científica. Direito Público, v. 16, n. 90, 2019.

DIMOULIS, Dimitri; MARTINS, Leonardo. Teoria Geral dos Direitos Fundamentais. 6. ed. São Paulo: Thomson Reuters Brasil, 2018.

FIGUEIRA, Vitor Pinheiro. "Internet das coisas": um estudo sobre questões de segurança, privacidade e infraestrutura. 2016.

GIL, Antonio Carlos. Como elaborar Projetos de Pesquisa. 4. ed. São Paulo: Atlas S.

A, 2002. 41 p. v. 3.

HINTZBERGEN, Jule et al. Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002. Brasport, 2018.

IDC. IoT Growth Demands Rethink of Long-Term Storage Strategies, Says IDC. <https://www.idc.com/getdoc.jsp?containerId=prAP46737220>, 2020.

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

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 13. São Paulo: Saraiva, 2018.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor-Linhas gerais de um novo direito fundamental. Saraiva Educação SA, 2017.

MAYMI, F.; HARRIS, S. Cissp all-in-one exam guide. 9. ed. Nova York: McGraw Hill, 2021.

MONTEIRO, Tiago Guimarães. Análise de requisitos de segurança para uma rede de IoT. 2021.

MORAES, Alexandre de; Direito constitucional. 35. ed. São Paulo: Atlas, 2019.

NOBRE, Jeferson 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, v. 17, n. 4, 2019.

OLIVEIRA, Mateus Souza et al. Aplicação das normas abnt nbr iso/iec 27001 e abnt nbr iso/iec 27002 em uma média empresa. Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica, v. 6, n. 2, 2016.

## Abordagem YOLOv5 para Detecção e Classificação de Esferas de Solda no Encapsulamento de Semicondutores

Resumo: A detecção de objetos baseada em visão computacional é essencial para acelerar a produção de produtos eletrônicos. Entretanto, a detecção automática de defeitos em superfícies de PCB ainda é uma tarefa desafiadora. Apesar da existência de diversos detectores baseados em visão computacional que abordam esses problemas, os detectores atuais enfrentam desafios para atingir alta precisão de detecção e velocidade. Para o treinamento e teste da rede neural, foram consideradas três métricas para avaliar os resultados da detecção: precisão, recall e mAP e para a classificação considerou-se a acurácia média. O objetivo consiste em propor uma abordagem para detectar e classificar três categorias de esferas de solda, no processo de soldagem de pastilhas de silício em BGA contidos em substratos PCB usando o modelo YOLOv5. Os resultados experimentais mostram que o detector alcançou um desempenho considerável, marcando um mAP@50 de 92,6% para o modelo YOLOv5.

Palavras-chave: Inteligência Artificial, Visão Computacional, YOLOv5, Semicondutores, Detecção de Objetos

### 1. Introdução/Justificativa

A produção de dispositivos de memória representa um grande desafio de fabricação em relação à dimensão dos componentes ser de tamanho ínfimo,

além de exigir alta precisão em sua operação. Nesse contexto, a inspeção de semicondutores tem a função de informar sobre os erros específicos de fabricação, que podem estar relacionados com problemas de produção. Assim sendo, a inspeção de semicondutores inclui a avaliação da ocorrência de falhas relacionadas aos materiais envolvidos nos processos ou definições inadequadas de parâmetros (Zhang et al., 2021).

Relatos apontam que as inspeções de qualidade continuam sendo realizadas em sua maioria por humanos. Apesar de profissionais qualificados, essas análises apresentam eficácia entre 80% e 90% dos casos (Silva et al., 2022). No entanto, esse processo manual é repetitivo e trabalhoso e sujeito a variações e fadigas. Na Figura 1, é apresentado um exemplo de inspeção visual humana de pastilhas de silício no qual o operador deve percorrer visualmente todos os componentes do substrato da Placa de Circuito Impresso (PCB) em busca de diversos tipos de defeitos, sendo, portanto, um processo desafiador em relação ao tamanho das esferas de solda e as características envolvidas na análise do problema.

Com os avanços da inteligência artificial, os algoritmos de aprendizagem profunda têm melhorado os resultados em diversas aplicações (Khan et al., 2020). Os referidos algoritmos podem ser usados

para obter uma inspeção mais confiável e eficiente em cenários altamente complexos. Em comparação aos métodos tradicionais, esses benefícios do aprendizado profundo motivam os pesquisadores a desenvolver algoritmos para analisar as imagens capturadas das fábricas e fornecer metodologias de inspeções inteligentes. Para este fim, a detecção de objetos tem atraído muita atenção nos últimos anos (Zhao et al., 2019).

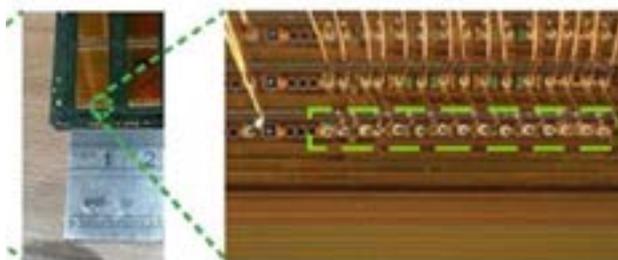
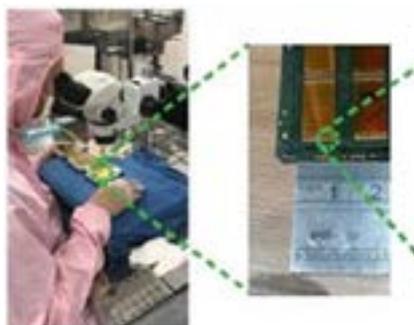


Figura 1. Inspeção visual convencional no processo de soldagem de pastilhas de silício

A detecção de objetos visa detectar um objeto em uma imagem, localizá-lo com uma caixa delimitadora e classificá-lo com a pontuação de confiança para a classe prevista. É um dos problemas fundamentais em aplicações de visão computacional e fornece informações valiosas (Cao et al., 2017). Além disso, a detecção de objetos

pode ajudar no processo de inspeção de fabricação, detectando o objeto desejado nos quadros de vídeo e decidindo se a inspeção foi realizada corretamente ou não.

## 2. Objetivo

Este estudo se propõe a colaborar na resolução do problema de inspeção automática no controle de qualidade do processo de soldagem de pastilhas de silício, chamados die, em BGA (do inglês, Ball Grid Array). Para isso, é apresentada uma abordagem para detectar e classificar esferas de solda em três categorias: i) Correta; ii) Falha; e iii) Ausente. Nesse processo foram utilizadas técnicas de visão computacional na detecção e classificação de regiões onde deveriam ser encontradas esferas de solda, utilizando uma Rede Convolucional da família YOLO (do inglês, You Only Look Once).

## 3. Metodologia

O problema de inspeção da qualidade de solda de placas PCB foi abordado no escopo deste trabalho como uma tarefa de detecção e classificação mediante aprendizado supervisionado com a arquitetura YOLO. A metodologia adotada neste trabalho é dividida em quatro etapas principais: i) Aquisição de imagens; ii) Pré-Processamento; iii) Detecção; e iv) Classificação. Por fim, com vistas ao objetivo de avaliar e comparar a performance do algoritmo YOLOv5 para detecção de objetos, algumas métricas de avaliação foram utilizadas. Cada etapa do desenvolvimento dessa pesquisa é

resumida no fluxograma apresentado na Figura 2.

A Figura 2 apresenta a visão geral sobre o processo de detecção automática de esfera de solda no processo de soldagem de pastilhas de silício em Ball Grid Array (BGA), contidas em um substrato de placas de circuito impresso. Inicialmente, um conjunto de imagens de pastilhas de silício é captado por uma câmera. Nessas imagens, são apresentadas três categorias para a análise da classificação: correta, ausente ou falha. Após a construção do banco de imagens, todas as imagens foram divididas em um conjunto de treinamento, um conjunto de validação e um conjunto de testes. Os conjuntos de treinamento e validação foram utilizados para o treinamento e o conjunto de testes foi usado para avaliação do modelo.

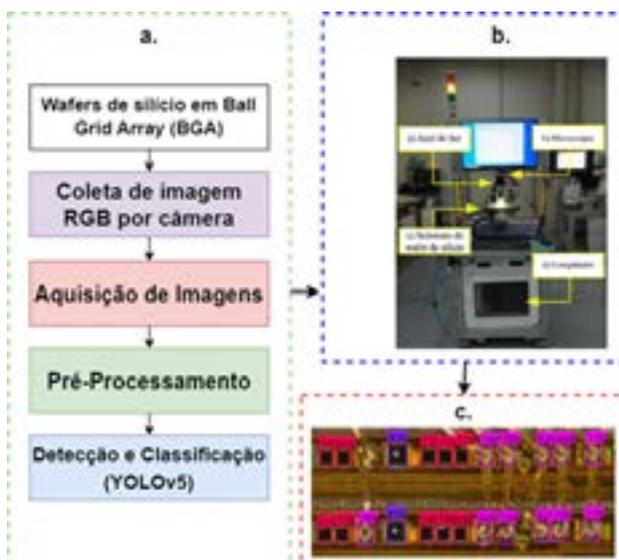


Figura 2. Método proposto. a) Fluxograma do processo experimental. b) Plataforma de captação de imagens. c) Imagens do resultado do processo de detecção usando o YOLOv5

### 3.1 Aquisição de Imagem

Esse processo consiste na captura de um conjunto de imagens adquiridas no modo Red, Green, Blue (RGB). Para isso, foi utilizado um dispositivo de aquisição de imagem, composto por um Estereomicroscópio Olympus SZ61TR, acoplado a uma câmera SC180. Essa estrutura dispõe de um sistema de iluminação que fornece luzes adequadas para a captura das imagens. Cada imagem capturada é encaminhada para o computador, de modo que seja processada posteriormente. A procedência das imagens originou-se do projeto de pesquisa e desenvolvimento do trabalho de (Silva et al., 2022) realizado em uma fábrica de componentes eletrônicos da Zona Franca de Manaus. O arcabouço experimental pode ser visualizado na Figura 2b.

### 3.2 Pré-Processamento de Imagem

A etapa de pré-processamento consiste em preparar as imagens das pastilhas de silício para realizar o treinamento do modelo YOLOv5. Para isso, as imagens foram redimensionadas para a resolução de 640x640 pixels, conforme as especificações da arquitetura YOLO disponível no repositório (Jocher et al., 2020). Em seguida, foi empregada a técnica de aumento de dados (do inglês, data augmentation), utilizando a ferramenta Roboflow (Alexandrova et al. 2015), para suplementar os dados de treinamento aplicando as operações de girar (verticalmente e horizontalmente), giro de

90°, cortar (para descartar aleatoriamente um subconjunto da imagem original), rotação aleatória, tesoura (para distorcer aleatoriamente a imagem original em seu eixo vertical ou horizontal), escala de cinza (8 bits), matiz, saturação, brilho, exposição (para ficar mais claro ou escuro), desfoque (borramento) e ruído aleatório.

Esse procedimento cria técnicas de aumento de dados para melhorar a diversidade do conjunto de treinamento e aprimorar a generalização do modelo (Sakkos et al., 2019). Cada imagem foi anotada utilizando a ferramenta Roboflow, construindo assim, uma coleção de referência com um total de 241 imagens para o conjunto de dados de treinamento e teste do modelo, conforme mostra a Figura 3. A Tabela 1 apresenta o número total de categorias anotadas. Em seguida, as imagens foram exportadas no formato YOLOv5 PyTorch.

Tabela 1. Número total de categorias anotadas por classe

Categorias	Quantidade
Correta	1444
Falha	646
Ausente	457
<b>Total</b>	<b>2547</b>

Figura 4. Arquitetura da rede YOLOv5s, destacando a função de cada subdivisão do modelo

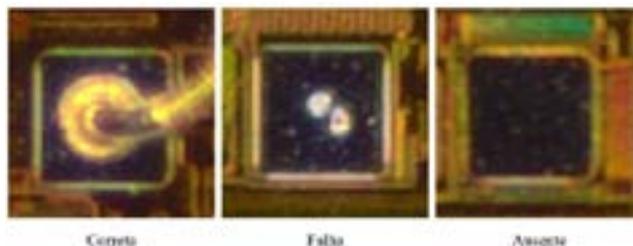


Figura 3. Amostra de imagens do conjunto de dados, dividido em Correta, Falha e Ausente

### 3.3 Detecção das Esferas de Solda (YOLOv5)

O YOLOv5 é a quinta versão da série You Only Look Once (YOLO) de algoritmos para detecção de objetos (Jocher et al., 2020). Assim como seus predecessores, é uma rede de detecção de estágio único que a torna mais rápida em comparação com outros algoritmos de detecção de objetos. O modelo de reconhecimento do YOLOv5 pode garantir alta precisão na velocidade de detecção em tempo real.

De acordo com o tamanho da profundidade da rede e a largura do gráfico de recursos, a variação Small (YOLOv5s) é adotada como modelo de uso (Jocher et al. 2016), constituída por cinco modelos que diferem no tamanho da rede neural e que possuem integração nativa com o framework PyTorch.

O modelo escolhido foi utilizado por dar ênfase nas três subdivisões principais da rede: i) Backbone: responsável por extrair características (features) da imagem; ii) Neck, onde são tratadas essas features para a etapa de detecção, agregando

e combinando as mesmas; e iii) Detect (também chamado de head) que é a etapa de detecção, onde possui como saída um vetor contendo os dados das detecções feitas (descrições das caixas delimitadoras)

resultando com as imagens e a localização do objeto de interesse formada. Na Figura 4, é apresentado o fluxo de dados entre essas três subdivisões.

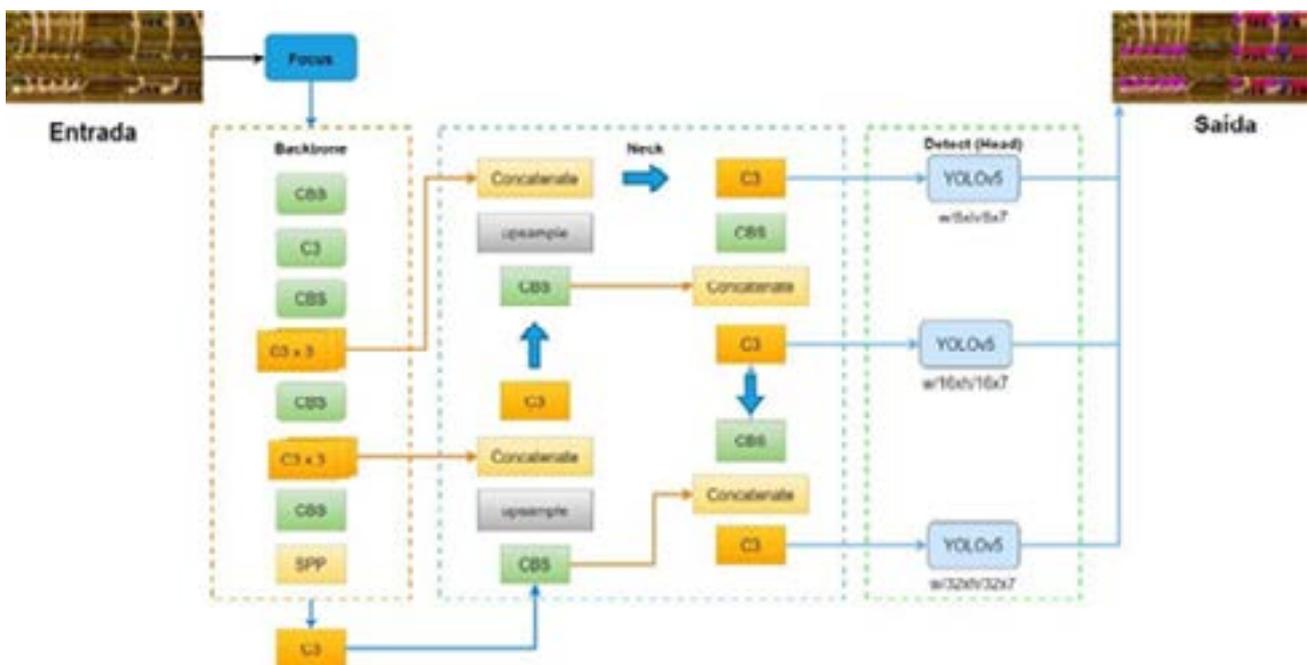


Figura 4. Arquitetura da rede YOLOv5s, destacando a função de cada subdivisão do modelo

Alguns hiperparâmetros significativos foram mantidos no estado padrão disponível no repositório, como o tamanho da entrada do modelo em três canais (RGB) de dimensões 640x640, o otimizador SGD, o limiar de Non-maximum Supression (NMS), responsável por evitar detecções múltiplas para um mesmo objeto, com valor de 0,45 e o limiar de confiança da detecção em 0,25.

A etapa de treinamento foi realizada na plataforma online Google Colab que disponibiliza uma máquina virtual com

placa de vídeo dedicada (GPU), que nesse caso foi uma Tesla T4. Os hiperparâmetros foram selecionados por meio de observação empírica, utilizando uma abordagem de tentativa e erro, além de considerar os valores padrões utilizados pelo método YOLOv5 na base de imagens COCO.

#### 4. Resultados

Nesta seção, apresenta-se o resultado e discussão do modelo treinado com o algoritmo YOLOv5 usando imagens e anotações da base de referência. A

seção discute as métricas de avaliação de desempenho do modelo.

#### 4.1 Avaliação das Detecções de Esferas de Solda (YOLOv5)

Os resultados obtidos para o conjunto de treinamento e validação são expostos na Tabela 2. Observando os resultados da tabela, é possível verificar o bom desempenho da arquitetura escolhida para a problemática levantada ao longo deste trabalho. A média dos valores de mAP@50 ficaram em 92,6%.

Tabela 2. Métricas obtidas ao final das 300 épocas de treinamento

Classe	Precisão	Recall	mAP@50	mAP50:95:100
Todas	83,6%	90,1%	92,6%	65,7%
Ausente	81%	91,6%	90,6%	63,3%
Correta	87,6%	90,6%	95,7%	67,7%
Falha	82,1%	88,3%	91,5%	66,1%

As métricas relevantes são mostradas na Figura 5. O processo de treinamento mostrou tendência decrescente de pontuação de perda de caixa normalizada ao longo das épocas para o conjunto de treinamento. A função de perda de caixa representa a precisão com que o algoritmo pode localizar o centro de um objeto (categoria de solda) e o quão bem a caixa

delimitadora prevista cobre um objeto. A perda de objetividade (obj\_loss) é uma medida da probabilidade de que um objeto exista em uma região proposta de interesse.

A Figura 5 também ilustra a tendência da pontuação de perda de caixa normalizada ao longo dos períodos de treinamento. A perda de caixa diminui ao longo da fase de treinamento no conjunto de treinamento e validação. Isso implica em um bom potencial de generalização do modelo YOLOv5s na localização de esfera de solda, falha de solda ou ausência de solda. A perda de objetividade no conjunto de validação apresentou tendência ascendente após 100 épocas, portanto o treinamento foi interrompido precocemente.

Os escores de precisão e recall diminuíram consistentemente durante o treinamento. Mais imagens no conjunto de dados podem potencialmente levar ao aumento da pontuação de recall. É possível notar como a pontuação de precisão e recall aumentaram ao longo das épocas de treinamento. O modelo treinado estava detectando as categorias de solda com precisão considerável.

A Figura 6 sintetiza o resultado das classificações para cada categoria por meio de uma matriz de confusão. Através dela observa-se que as categorias foram detectadas com uma taxa considerável de precisão.

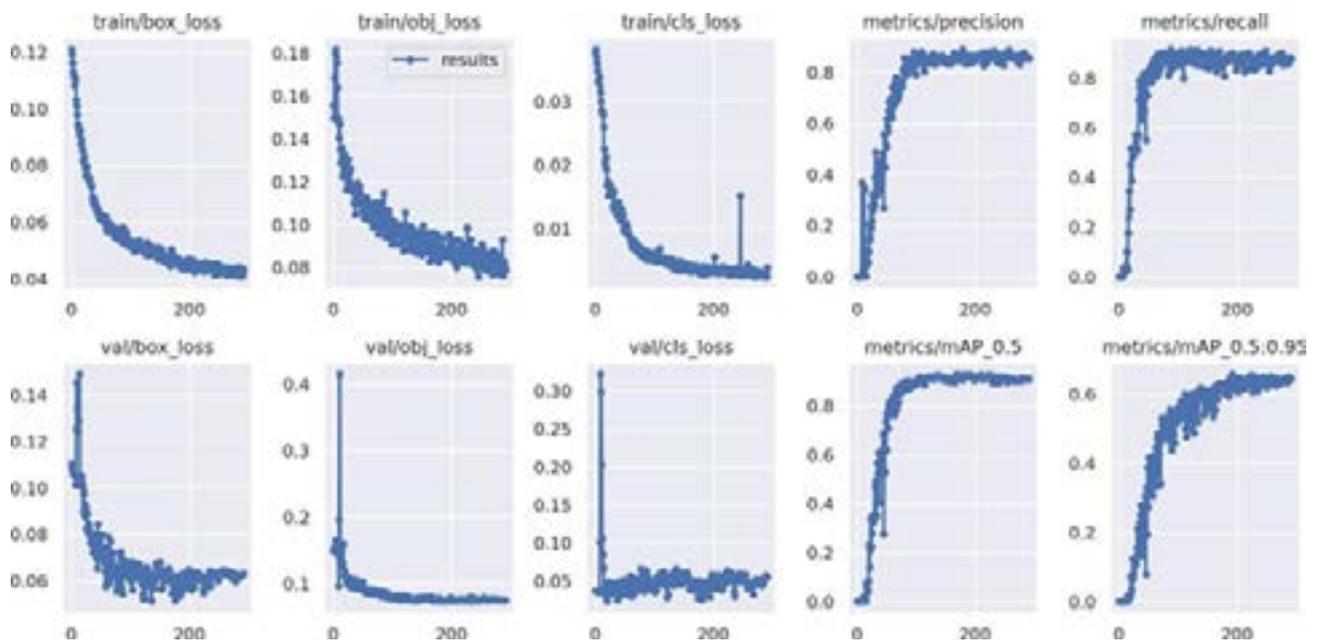


Figura 5. Visão geral dos resultados do treinamento do modelo baseado no detector YOLOv5s. Os gráficos ilustram a curva da função de perda para três diferentes variáveis, considerando tanto o conjunto de treinamento (train), quanto o conjunto de validação (val)

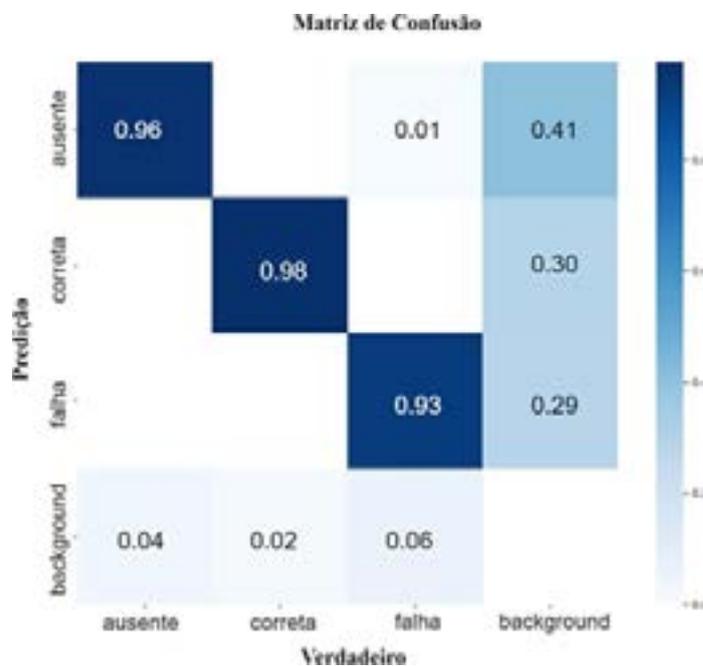


Figura 6. Matriz de confusão das detecções obtidas no conjunto de treinamento

A fim de ilustrar o desempenho do modelo, uma comparação entre as imagens de treinamento e teste é mostrada na Figura 8. Esta figura compara os dados utilizados no treinamento do modelo, manualmente rotulados, com as previsões desempenhadas nestes mesmos dados. Observa-se que o modelo detectou as

três categorias propostas neste estudo. Tal desempenho retrata a capacidade do modelo de aprender, com relativa eficácia, os padrões necessários para caracterizar uma esfera de solda com base no conjunto de dados fornecidos, justificando a precisão e o recall obtidos durante o treinamento.

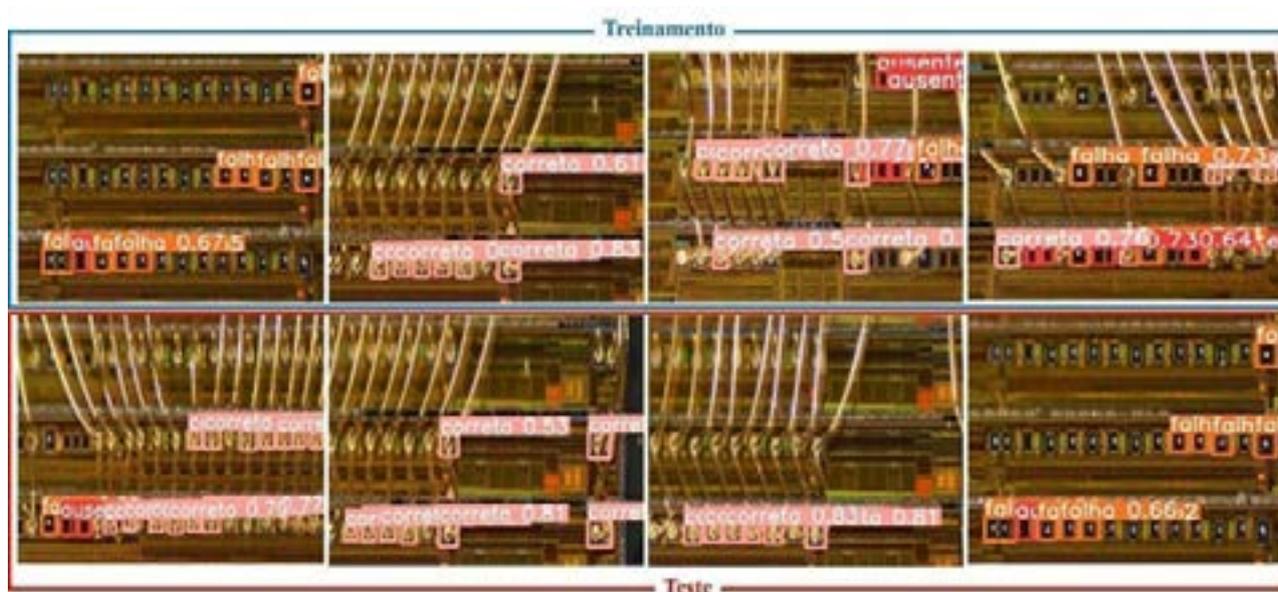


Figura 8. Performance do modelo nos dados utilizados para o treinamento e teste

## 5. Considerações Finais

O trabalho em questão abordou o problema de inspeção visual de soldagem no encapsulamento de semicondutores. A principal contribuição do presente trabalho foi fornecer uma abordagem para detectar e classificar categorias de esferas de solda de três classes de objetos. Ao contrário de outras metodologias, o método proposto atinge alta precisão e apresenta grande capacidade de inspecionar condições de esferas de solda muito pequenas, proporcionando melhoria no processo

de encapsulamento e produção de semicondutores.

O modelo de rede neural YOLOv5, para a tarefa de detecção, alcançou precisão de 83,6%, recall de 90,1% e mAP@50 de 92,6%. Esses resultados são considerados satisfatórios, considerando a base de imagens utilizada nos experimentos. As imagens das pastilhas de silício continham muitos objetos com propriedades de cor ou textura semelhantes às categorias de soldas propostas neste estudo.

A partir dos resultados obtidos, verificou-se que o modelo treinado alcançou notável capacidade de generalização frente às categorias de objetos proposta neste estudo. Como limitações, não foi possível realizar uma comparação justa para o desempenho do modelo YOLOv5 frente a outros modelos de detecção. Por fim, nessa linha de pesquisa, trabalhos futuros podem ser realizados tomando como ponto de partida o estudo comparativo realizado com a arquitetura YOLO. Também pretende-se concentrar esforços para estender a abordagem de inspeção visual automática para lidar com outros tipos de problemas relacionados ao encapsulamento de semicondutores. A análise e inspeção das ligações dos fios também é um problema relevante para investigação e se faz necessário incorporar nas linhas de produção. O repositório deste trabalho, juntamente com o dataset utilizado, encontra-se disponível nas referências (PEREIRA, 2022).

## Referências

Zhang, K., Huang, T., Su, Z., and Guan, T. (2021). **Design of solder quality inspection system based on machine vision**. In 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), volume 5, pages 2413–2418.

Silva, C., Ferreira, N., Meireles, S., Otani, M., Silva, V., Freitas, C., and Oliveira, F. (2022). **The visual inspection of solder balls in semiconductor encapsulation**. Pages 750-757.

Khan, A., Sohail, A., Zahoor, U., and Qureshi, A. S. (2020). **A survey of the recent architectures of deep convolutional neural networks**. Artificial intelligence review, 53(8):5455–5516.

Zhao, Z.-Q., Zheng, P., Xu, S.-t., and Wu, X. (2019). **Object detection with deep learning: A review**. IEEE transactions on neural networks and learning systems, 30(11):3212– 3232.

Cao, Y. (2021). **Design and application of robot vision inspection system for semiconductor metal target**. In 2021 3rd International Symposium on Robotics Intelligent Manufacturing Technology (ISRIMT), pages 464–467.

Jocher, G., Nishimura, K., Mineeva, T., and Vilarino, R. (2020a). **Yolov5** (2020). GitHub repository: <https://github.com/ultralytics/yolov5>.

Alexandrova, S., Tatlock, Z., and Cakmak, M. (2015). **Roboflow: A flow-based visual programming language for mobile manipulation tasks**. In 2015 IEEE International Conference on Robotics and Automation (ICRA), pages 5537–5544. IEEE.

Zhou, J. G., Chen, H., Long, Y., Wang, K., Guo, H., and Liu, F. (2021). **Backside defect monitoring strategy and improvement in the advanced semiconductor manufacturing**. In 2021 China Semiconductor Technology International Conference (CSTIC), pages 1–5.

PEREIRA, P. V. L. **Página do repositório do código deste projeto**. 01/2022. Disponível em: <https://github.com/paulovitor21/tcc-soldering-balls>.

# DIREITO FUNDAMENTAL À PRIVACIDADE E À PROTEÇÃO DOS DADOS PESSOAIS: UMA ANÁLISE FRENTE AO DESENVOLVIMENTO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL

## RESUMO

Nas últimas décadas, tem se observado um crescente desenvolvimento tecnológico, principalmente, no que concerne às Tecnologias de Informação e Comunicação, com destaque para o desenvolvimento da Inteligência Artificial (IA) e das suas implicações éticas, sociais e jurídicas. Diante disso, o presente trabalho tem como objetivo analisar os impactos da Inteligência Artificial sobre o direito fundamental à privacidade e à proteção dos dados pessoais, tendo como objeto de estudo a investigação do direito fundamental à privacidade e à defesa dos dados pessoais, sua origem, características e legislações concernentes, frente ao desenvolvimento da Inteligência Artificial. Desse modo, para elaboração do presente trabalho, utilizou-se a pesquisa bibliográfica, documental, e a análise de casos concretos a respeito do tema proposto, por meio de uma abordagem qualitativa dos dados coletados e levando em consideração a pesquisa predominantemente exploratória sobre o tema analisado. Assim, concluiu-se, ainda que de maneira introdutória sobre o tema, a necessidade de uma maior regulamentação e análise sobre o assunto, a fim de promover o desenvolvimento de uma IA de confiança, a qual respeite

os direitos fundamentais, com destaque à proteção da privacidade e dos dados pessoais.

**Palavras-chave:** inteligência artificial, privacidade e dados pessoais.

## ABSTRACT

In recent decades, there has been a growing technological development, mainly with regard to Information and Communication Technologies, with emphasis on the development of Artificial Intelligence (AI) and its ethical, social and legal concerns. In view of this, the present work aims to analyze the impacts of Artificial Intelligence on the fundamental right to privacy and protection of personal data, having as its object of study the investigation of the fundamental right to privacy and the defense of personal data, its origin, characteristics and legislation concerning the development of Artificial Intelligence. Thus, for the elaboration of this work, bibliographical and documental research and the analysis of concrete cases regarding the proposed theme were used, through a careful approach to the collected data and taking into account the

<sup>1</sup> Acadêmica do Curso de Direito da Universidade do Estado do Amazonas (UEA). E-mail: rdln.dir22@uea.edu.br.

predominantly exploratory research on the theme. treaty . Thus, it is concluded, even if in an introductory way on the subject, the need for greater regulation and analysis on the subject, in order to promote the development of a reliable AI, which respects fundamental rights, with emphasis on the protection privacy and personal data.

**Keywords:** artificial intelligence, privacy and personal data.

## INTRODUÇÃO

Desde o advento da internet na década de 60, juntamente com o intenso desenvolvimento das Tecnologias de Informação e Comunicação (TICs) nos anos que se sucederam, o número de dados de empresas, órgãos públicos e cidadãos comuns disponíveis no ambiente on-line atingiu proporções inimagináveis. Esse fator, aliado a criação da computação em nuvem, big data, juntamente com outras tecnologias, permitiu o surgimento da Inteligência Artificial (IA) – tecnologia utilizada para o auxílio no manuseio de informações e na execução de tarefas de forma cada vez mais aprimorada, por meio da análise de dados dos usuários.

Entretanto, não obstante muitos sejam os benefícios dessa tecnologia, nota-se hodiernamente a necessidade da análise sobre os impactos desta no que tange aos direitos fundamentais, em especial ao direito à privacidade e à proteção dos dados

personais, tendo em vista o grande volume de dados disponibilizados diariamente por empresas, usuários e repartições públicas no ambiente on-line, sem muitas vezes se ter noção de como, para quê e por quem serão utilizados esses dados. Dessa forma, faz-se necessário analisar tal processo, a fim de compreender melhor os impactos da inteligência artificial sobre o direito à privacidade e à proteção dos dados pessoais, de forma a colaborar para o desenvolvimento de uma IA confiável. Diante disso, o objeto de análise da presente pesquisa será a proteção do direito fundamental à privacidade e aos dados pessoais, diante do avanço da Inteligência Artificial.

## JUSTIFICATIVA

No que concerne à perspectiva brasileira, nos últimos anos, tem-se observado um crescente desenvolvimento da IA no país. Hodiernamente, ela pode ser encontrada nos aplicativos de mobilidade e de comunicação, como o aplicativo Waze, por exemplo, e chatbots de empresas, respectivamente; nos sistemas de reconhecimento facial de segurança, bem como nos processos de otimização e de processamento de dados em bancos e instituições financeiras, dentre outras aplicações, como para o diagnóstico de doenças na área da saúde.

Entretanto, embora o desenvolvimento da IA traga grandes benefícios para o ser humano, sendo

fundamental no auxílio na produtividade e na eficiência das atividades humanas, nota-se que o seu emprego também pode gerar prejuízos para os indivíduos, principalmente no que concerne à violação do direito à privacidade e à proteção dos dados pessoais. Logo, sendo necessário pensar em princípios e mecanismos para produção de uma IA segura.

Nesse sentido, o presente trabalho visa analisar tal ocorrência no Brasil, com base até mesmo em casos internacionais, e suas possíveis consequências, a fim de discutir ações para mitigar tal problemática. Para isso, primeiramente, serão apresentados os conceitos basilares relacionados aos direitos fundamentais. Por conseguinte, relacionados à IA e aos princípios que a regem, para então, discutir alguns casos concretos sobre o tema ocorridos no Brasil e em âmbito internacional, assim como seus impactos, a fim de que ações sejam tomadas para mitigação da problemática, principalmente, sob a óptica jurídica.

## **1 CONCEITOS INTRODUTÓRIOS DOS DIREITOS FUNDAMENTAIS**

Primeiramente, ao tratar acerca dos direitos fundamentais, é primordial a compreensão de algumas definições introdutórias sobre o tema, a fim do melhor entendimento sobre o assunto e de como ele têm sido impactados pela IA. Dessa

forma, acerca do tema, Bonavides (2020) descreve, utilizando-se dos ensinamentos de Carl Schmitt, que os direitos fundamentais, do ponto de vista formal, podem ser caracterizados pela sua presença no instrumento constitucional, sendo aqueles que “receberam da Constituição um grau mais elevado de garantia ou de segurança”, culminando na dignidade da pessoa humana, do ponto de vista material. Nesse mesmo sentido, Canotilho (2003) afirma sobre esse processo de afirmação dos direitos fundamentais que consiste na “incorporação de direitos subjetivos do homem em normas formalmente básicas, subtraindo-se o seu reconhecimento e garantia à disponibilidade do legislador originário”.

Dessa forma, os direitos fundamentais são aqueles positivados no ordenamento constitucional de cada Estado em determinado momento histórico e que carecem da proteção e da efetivação na prática concreta da sociedade ali inserida, por meio da atuação dos entes estatais. A esse respeito, nota-se que a evolução dos direitos fundamentais percorreu um longo caminho até chegar a forma como se conhece hoje, assim, embora não seja o objetivo deste trabalho, é importante destacarmos na Idade Antiga os conflitos entre direito natural, direito divino e o relativismo, já na Idade Média, tem-se como marco a Magna Carta (1215), assinada pelo rei João Sem Terra, que, conquanto não fosse uma declaração de direitos, por apenas conceder privilégios aos nobres

ingleses, representou uma das primeiras marcas de limitação do poder soberano, bem como de afirmação de direitos a determinados indivíduos, por meio de um documento legislativo.

Na Idade Moderna, tem-se como grande marco a Bill of Rights (1689) – carta de direitos criada pelo Parlamento Inglês. Por fim, na idade contemporânea, tem-se como destaque a Declaração Universal dos Direitos Humanos de 1948 que vem para reafirmar um conjunto de direitos, esquecidos pelas barbáries cometidas durante a Segunda Guerra Mundial.

No que concerne à realidade brasileira, eles estão positivados na Constituição Federal de 1988, conhecida como Constituição Cidadã, com destaque para o rol taxativo presente no Título II que trata “Dos Direitos e Garantias Fundamentais”. Ademais, dividem-se em direitos de primeira geração – direitos de liberdade –, os quais exigem do Estado, de forma geral, um status negativo, de não intromissão; os direitos de segunda geração - direitos de igualdade – que reivindicam pela igualdade material e exigem do Estado uma prestação positiva, bem como os direitos de terceira geração – direitos de solidariedade ou fraternidade –, voltados não mais para um indivíduo ou grupo específico, mas para a sobrevivência do gênero humano.

Nesse diapasão, o direito à privacidade e à proteção dos dados pessoais classificam-se na primeira

geração mencionada – direitos de liberdade –, tendo em vista terem como destinatários o indivíduo em si e suas liberdades fundamentais - privacidade e dados pessoais.

### **1.1 Direito fundamental à privacidade**

No que concerne ao direito à privacidade, é importante explicitar que este encontra-se previsto no rol de direitos fundamentais presentes na Constituição Federal de 1988, respectivamente no art. 5º, inciso X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas...”. Ademais, o direito à privacidade também é tratado, em especial no art. 16 ao 21, da Lei nº 10.406 de 2002, intitulada Código Civil, na parte que discorre acerca dos direitos da personalidade. Bem como, em âmbito internacional, a Declaração Universal dos Direitos Humanos de 1948, afirma que:

Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948, p. 3).

A esse respeito, Gonçalves (2017) esclarece que o direito à privacidade é o “direito que um indivíduo tem de se destacar

(se separar) de um grupo, isolando-se da observação dele ou como, ainda, o direito ao controle das informações veiculadas sobre si mesmo”. Dentro dessa perspectiva, tem-se como marco inicial, no que tange à análise da privacidade sob o panorama jurídico, o artigo *The Right To Privacy*, dos autores Samuel Warren e Louis Brandeis, no qual eles entenderam a privacidade como o “direito de ser deixado só”, em outras palavras, o direito de ser esquecido, e de tal esquecimento ser respeitado pelos demais, inclusive no que concerne a sua intimidade e vida privada. Desse modo, trata-se de um direito, por muito tempo considerado extrínseco ao indivíduo, ligado à propriedade, mas que, ao longo dos anos, passou a ser considerado intrínseco a ele, ligado à tutela da personalidade humana. (MAGALHÃES; OLIVEIRA, 2021).

Nesse diapasão, conquanto não haja um consenso doutrinário sobre o assunto, estabelecer-se-á no presente trabalho a distinção entre “privacidade” e “intimidade” para uma melhor compreensão sobre o assunto. Com relação ao primeiro, Gonçalves (2017), menciona que é o espaço no qual “se estabelecem os relacionamentos familiares, de lazer, negócios, amorosos” e a vida privada refere-se a um “núcleo ainda menor, que perpassa e protege relações mais íntimas ou pessoais”.

Dessa forma, na contemporaneidade, com o desenvolvimento das TICs, é preciso pensar não somente mais em privacidade

no espaço familiares físicos, entre amigos, no trabalho, na academia, nas atividades in loco do dia a dia. Mas é preciso compreendê-la, principalmente, no ambiente virtual, no qual, cada vez mais, têm-se as informações pessoais compartilhadas, locais no qual o usuário esteve compartilhado, fotos, imagens postadas e disponíveis para diversos usuários, constituindo assim um novo paradigma a ser pensado. Nesse entendimento, Doneda destaca:

a tecnologia operou especificamente a intensificação dos fluxos de informação e, conseqüentemente, de suas fontes e seus destinatários. Tal mudança, a princípio quantitativa, acaba por influir qualitativamente, mudando os eixos de equilíbrio na equação entre poder – informação – pessoa – controle. Isto implica que identifiquemos uma nova estrutura de poder vinculada a esta nova arquitetura informacional. (DONEDA, 2006, p. 10)

A partir desse cenário, vê-se o quanto a tecnologia tem transformado as relações sociais, não somente no que tange a quantidade cada vez maior de aparatos tecnológicos, mas principalmente no que concerne à superexposição propiciada por esse desenvolvimento tecnológico, impulsionando assim a Sociedade em Rede. Entretanto, como mencionado acima, observa-se que esse desenvolvimento deve ser acompanhado da atenção sobre as possíveis implicações

sociais e jurídicas quanto à utilização dessas tecnologias, tendo em vista que o direito à privacidade passou por um longo processo de lutas até sua afirmação e deve ser respeitado, bem como analisado, a fim de que haja uma compreensão clara sobre o tema e de que se evite uma “neutralização” dos impactos tecnológicos sobre a sociedade, acreditando-se que, aos poucos, os indivíduos tendem a perder sua privacidade, quando, na verdade, esta continua sendo afirmada como direito fundamental no ordenamento constitucional brasileiro e nas declarações internacionais. Todavia, tendo como base que o direito à privacidade não é um direito absoluto e tem limitações como a tutela de outros direitos fundamentais, como a liberdade de expressão e o acesso à informação pública, ou o interesse público.

## **1.2 Direito fundamental à proteção dos dados pessoais**

A partir disso, no que concerne ao direito à proteção dos dados pessoais, nota-se que ele se encontra intimamente relacionado ao direito à privacidade, uma vez que é quase inviável tratar sobre os dados pessoais sem levar em conta que se tratam de elementos básicos inerentes ao indivíduo e à personalidade humana – ou seja – inerentes a sua privacidade.

Dessa forma, no que diz respeito à legislação brasileira, a proteção dos dados pessoais encontra-se prevista

na Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, [...] com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”. Desse modo, tratando-se de importante marco no que se refere ao tratamento dos dados pessoais no Brasil.

Já em 2022, a Emenda Constitucional nº 115, acrescentou tal proteção a nível constitucional, conforme se lê no art. 5º, LXXIX, CF/88: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”. Sob esse assunto, Sarlet (2022) afirma “o fato é que sua positivação formal, em sendo o caso, carrega consigo uma carga positiva adicional, ou seja, agrega (ou, ao menos, assim o deveria) valor positivo substancial em relação ao atual estado da arte no Brasil”. Assim, para melhor discussão sobre o tema, utilizar-se-á alguns conceitos previstos na LGPD, os quais lê-se:

1) dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

2) 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;

3) banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

4) titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

5) controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

6) tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

7) consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

A partir dessas observações, nota-se a importância do consentimento do titular para o tratamento dos dados pessoais, e, principalmente, dos seus dados pessoais sensíveis, uma vez que essas informações estão intimamente relacionadas à privacidade do usuário, àquilo que lhe é característico. Desse modo, ao se estabelecer a proteção

desses elementos, estabelece-se também a proteção da privacidade do indivíduo frente às diversas esferas de interesse da sociedade contemporânea e, em última análise, sob as ameaças do capitalismo de vigilância .

Nesse diapasão, é possível concluir que o direito à proteção dos dados pessoais, hodiernamente, encontra-se previsto e resguardo a nível constitucional-fundamental, ou seja, carece de especial atenção, principalmente no que é relativo à sua proteção e tratamento frente aos meios digitais. Isso porque a sua utilização sem o consentimento do usuário, salvo os casos previsto em lei, constitui ato ilícito e atentatório aos direitos fundamentais.

## 2 INTELIGÊNCIA ARTIFICIAL E CONCEITOS INTRODUTÓRIOS SOBRE O TEMA

O termo “Inteligência Artificial” começou a ser desenvolvido na década de 50 e, em 1956, um grupo de estudiosos sobre o assunto se reuniram em uma conferência no Dartmouth College, nos Estados Unidos, onde John McCarthy se referiu ao termo como “a ciência e a engenharia de produzir máquinas inteligentes” (COSTA, 2021). Tempos depois, termos como machine learning e deep learning, mais recentemente, foram acrescentados para tratar sobre o tema. O primeiro termo, conhecido como “aprendizado de

máquina”, refere-se a uma técnica que permite o aperfeiçoamento do sistema com base nos dados fornecidos anteriormente a ele, ou seja, tendo como parâmetro as informações fornecidas ao sistema inicialmente, este consegue se aperfeiçoar (OLIVEIRA, 2018). Tem-se como exemplo o aplicativo já citado Waze, que, por meio da verificação de informações fornecidas sobre o trânsito pelos algoritmos, indica ao motorista o melhor trajeto a ser seguido.

Já o *deep learning*, também conhecido como aprendizagem profunda, segue na mesma linha de raciocínio da aprendizagem de máquina, entretanto, é capaz de realizar atividades mais complexas, como detecção de fala, de objetos e reconhecimento facial.

Nesse sentido, embora não haja uma definição única a respeito do termo, é oportuno conceituar o que se entende por Inteligência Artificial (IA) na contemporaneidade. Sob esse âmbito, de acordo com o grupo de especialistas de alto nível em IA da União Europeia (HIGH-LEVEL EXPERT GROUP ON AI, 2019, p. 8)

Sistemas de Inteligência Artificial (IA) são sistemas de software (e possivelmente também de hardware) projetados por

seres humanos que, dado um objetivo complexo, atuam na dimensão física ou digital, percebendo seu ambiente por meio da aquisição de dados estruturados ou não estruturados coletados, raciocinando sobre o conhecimento, ou processando as informações, derivadas desses dados e decidindo a(s) melhor(es) ação(ões) a ser(em) tomada(s) para atingir o objetivo determinado. Os sistemas de IA podem usar regras simbólicas ou aprender um modelo numérico, e também podem adaptar seu comportamento analisando como o ambiente é afetado por suas ações anteriores.

Dessa forma, observamos que se tratam de tecnologias, sistemas desenvolvidos para o auxílio dos seres humanos em suas atividades, por meio do manejo de algoritmos e tecnologias de machine e deep learning. Diante disso, Burle e Cortiz (2020) realizaram um mapeamento multissetorial, com base em iniciativas da Comissão Europeia, do Departamento de Defesa Norte-americano, Google, Microsoft, Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e da Academia de Inteligência Artificial de Pequim, para estabelecer os princípios básicos relacionados ao desenvolvimento, à implantação e à utilização da Inteligência

<sup>2</sup>Expressão cunhada pela professora Shoshana Zuboff para tratar acerca de uma nova fase do capitalismo moderno, marcada pela comercialização da experiência humana, bem como de seus dados, por meio de práticas de vigilância, principalmente, no que concerne ao ambiente digital. Para saber mais: <https://outraspalavras.net/tecnologiaemdisputa/origem-limites-do-capitalismo-de-vigilancia/>.

Artificial. No documento divulgado pelo NIC.br, sem o objetivo de ser exaustivo, foram destacadas as seguintes dimensões que devem ser consideradas para o desenvolvimento de uma IA confiável: equidade (fairness); confiabilidade e segurança (reliability & safety); impacto social (social impact); responsabilidade (accountability); privacidade & segurança (privacy & security); e transparência (transparency).

Desse modo, na contemporaneidade, a presença da IA tem sido uma realidade cada vez mais frequente no cotidiano dos indivíduos. Por meio do acesso aos dados corretos, os algoritmos tomam decisões, disponibilizam conteúdos de acordo com as preferências humanas e preveem padrões (RISSE, 2018). Todavia, em muitos casos, o desenvolvimento da IA pode trazer sérios riscos para os indivíduos, principalmente no que concerne aos seus direitos, devido a suas implicações sociais, éticas e jurídicas (GORZONI, 2019).

### **3 IMPACTOS DA INTELIGÊNCIA ARTIFICIAL SOBRE O DIREITO FUNDAMENTAL À PRIVACIDADE E À PROTEÇÃO DOS DADOS PESSOAIS**

Nos últimos anos, como já destacado anteriormente, muitas têm sido as aplicações da IA na vida dos indivíduos.

A filtragem utilizada pelo Google para personalização do seu feed de notícias, bem como para o resultado de buscas mais parecidas com os interesses dos usuários, a personalização utilizada pela Netflix para adequar os conteúdos ofertados pela plataforma de acordo com as preferências e desejos dos assinantes, os assistentes virtuais, como Siri e Alexa, as máquinas inteligentes utilizadas por médicos em cirurgias, dentre outras atividades que ao longo dos anos têm sido propiciadas e facilitadas pelo uso da IA.

Entretanto, para além dos benefícios proporcionados pelo uso da IA, tem-se observado casos cada vez mais recorrentes de violação dos direitos fundamentais. Nessa perspectiva, de acordo com um Relatório realizado pela empresa de segurança digital Kaspersky e publicado em 2022, durante a pandemia, empresas sofreram mais que o dobro de tentativas de ataques cibernéticos em comparação a 2019 – dados da pesquisa coletados até novembro de 2021. Dessa forma, com propósito exemplificativo, nota-se o caso da Cambridge Analytica, no qual, em 2014, a empresa americana teve acesso aos dados de mais de 50 milhões de usuários do Facebook sem o consentimento dos seus titulares. Já no Brasil, em 2019, informações de cerca de 2 milhões de clientes da empresa Netshoes

<sup>3</sup> Núcleo de Informação e Coordenação do Ponto BR - NIC.Br. Para saber mais: <https://nic.br/>.

foram expostas na internet, após falhas no sistema da empresa.

Nesse sentido, uma pesquisa realizada pelo Cetic.br, intitulada “Privacidade e Proteção de Dados Pessoais 2021”, mostrou que aproximadamente um quarto dos usuários de Internet (24%) procuraram por canais de atendimento para solicitações, reclamações ou denúncias sobre seus dados pessoais. Sob esse âmbito, 67% dos usuários se mostraram preocupados ou muito preocupados com compras on-line, por exemplo.

Ademais, com relação aos órgãos governamentais, observa-se que, muitos deles precisam da utilização de informações pessoais para realização de análises e armazenamento em bancos de dados. Todavia, torna-se fundamental que, embora de interesse público, os indivíduos tenham conhecimento sobre como os seus dados estão sendo tratados (transparência) e de que estes não serão utilizados para fins privados e de discriminação (equidade, confiabilidade e segurança).

Outrossim, sob o aspecto pessoas e empresas, nota-se que, cada vez mais, os dados dos usuários são disponibilizados no ambiente on-line para realização de compras, reserva de viagens e hotéis, navegação na Internet, dentre outros rastros deixados no ciberespaço. Nesse sentido, o estudo “Startups e o uso de Inteligência

Artificial: o impacto e o futuro da IA no Brasil”, realizado pelo Google for Startups, em parceria com a Associação Brasileira de Startups e a Box1824, mostrou que o país possui um cenário propício para o fomento da IA. Entretanto, questões como a falta de conhecimento e de inovação no setor, há baixa cultura de organização de dados, bem como a própria desconfiança da sociedade em tal tecnologia e a falta de letramento tecnológico, são fatores que colaboram para o distanciamento da IA das empresas e do cidadão comum.

Sob esse cenário, verifica-se a importância dos investimentos na capacitação de profissionais da área, com o auxílio de programas que promovam maior inclusão desses profissionais em empresas nacionais e que incentivem o desenvolvimento deles, de modo a criar uma cultura interna nacional de valorização do conhecimento científico e de compartilhamento de experiências, bem como de uma atuação pautada em princípios éticos.

Ademais, sob o aspecto cultural-social, observa-se importante a propagação de conhecimentos sobre a IA em escolas e universidades. Além disso, verifica-se a necessidade de diretrizes claras sobre como serão tratados os dados pessoais dos usuários por parte das empresas e aplicativos de tecnologia, bem como que

<sup>4</sup> Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – Cetic.br. Para mais informações: <https://www.cetic.br/>.

haja seu consentimento e que seus dados pessoais sensíveis sejam preservados.

Desse modo, conforme as “Orientações éticas para uma IA de confiança”, da Comissão Europeia, é fundamental o desenvolvimento, a implementação e a utilização de uma IA de confiança, por parte de desenvolvedores, controladores e titulares dos dados pessoais, a qual pode ser alcançada por meio de uma IA que seja ética, legal e sólida.

## CONSIDERAÇÕES FINAIS

Portanto, ao realizar o presente trabalho, teve-se como objetivo a análise das implicações do desenvolvimento da Inteligência Artificial sobre os direitos fundamentais, em especial, no que concerne ao direito fundamental à privacidade e à proteção dos dados pessoais. Desse modo, por meio da investigação bibliográfica documental e da análise de casos concretos, buscou-se identificar quais as relações estabelecidas entre esses elementos, bem como seus principais impactos, principalmente, com relação à violação dos direitos fundamentais dos indivíduos.

Dessa forma, foi realizado um levantamento histórico acerca dos direitos fundamentais, assim como acerca da atual positivação no ordenamento constitucional do direito à privacidade e à proteção dos dados

pessoais. Posteriormente, foi analisado os elementos primordiais relacionados à IA, como o conceito de machine learning e deep learning, bem como seu conceito utilizado na contemporaneidade, para fins de melhor compreensão sobre o tema estudado, conquanto não haja consenso sobre o assunto. Nesse sentido, também se apresentou alguns princípios básicos – ainda que não exaustivos – que devem nortear o desenvolvimento, a implementação e a utilização da IA de forma confiável.

Por fim, discutiu-se algumas das principais implicações e casos relacionados à utilização da IA que vão de encontro aos direitos fundamentais supramencionados, principalmente, no que concerne às relações entre órgãos governamentais e pessoas, bem como às relações estabelecidas entre empresas e pessoas no ambiente on-line.

Desse modo, sem o fito de esgotar a discussão sobre o tema, bem como tendo em vista o caráter introdutório do presente trabalho acerca do tema proposto, concluiu-se que, na contemporaneidade, a IA tem trazido intensos questionamentos e implicações no que concerne à privacidade e à proteção dos dados pessoais. Todavia, observa-se, por vezes, a tentativa de naturalizar a discussão sobre o tema, como uma questão que, aos poucos, será incorporada na sociedade. Entretanto, entendeu-se a necessidade de aprofundar o estudo no tema proposto, a fim de entender mais profundamente as consequências

negativas da IA sobre os direitos fundamentais, bem como os mecanismos para evitar que tal situação ocorra. Ademais, observou-se a necessidade de uma discussão multissetorial, com a participação da sociedade, dos setores privados, do governo, do setor jurídico, dentre outros, com o objetivo de desenvolver ações para mitigar tal problemática e auxiliar na construção de uma IA que beneficie a todos, seja confiável e respeite os direitos fundamentais.

## Referências

ALMEIDA MAGALHÃES, R; OLIVEIRA, E. C. R. N. **O direito à privacidade na era digital**. Revista Jurídica da FA7, v. 18, n. 1, p. 55-70, 28 jun. 2021.

ARAGÃO, Alexandre. 5 grandes vazamentos de dados no Brasil — e suas consequências. **JOTA**, 2022. Disponível em: <https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022>. Acesso em: 27, dez. 2022.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 35<sup>a</sup> ed. Salvador, BA: Malheiros Editores/Juspodivm, 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Disponível em: [https://www2.camara.leg.br/atividade-legislativa/legislacao/constituicao1988/arquivos/ConstituicaoTextoAtualizado\\_EC%20127\\_128.pdf](https://www2.camara.leg.br/atividade-legislativa/legislacao/constituicao1988/arquivos/ConstituicaoTextoAtualizado_EC%20127_128.pdf). Acesso em: 21 dez. 2022.

\_\_\_\_\_. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

\_\_\_\_\_. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral DE Proteção De Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm#art65](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65). Acesso em: 15 mar. 2023.

BURLE, Caroline; CORTIZ, Diogo. **Mapeamento de princípios de inteligência artificial [livro eletrônico]**. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2020.

BRANDEIS, Louis D. WARREN, Samuel D. **The right to privacy**. In: Harvard Law Review, vol. 4, n. 5, dec. 15, 1890.

CANOTILHO, J.J. Gomes. **Direito Constitucional E Teoria Da Constituição**. 7. ed. Coimbra: Almedina, 2003. 378 p.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Privacidade e proteção de dados pessoais 2021** [livro eletrônico]: perspectivas de indivíduos, empresas e organizações públicas no Brasil. Núcleo de Informação e Coordenação do Ponto BR. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: [https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade\\_protecao\\_de\\_dados\\_pessoais\\_2021\\_livro\\_eletronico.pdf](https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf). Acesso em: 20 dez. 2022

COSTA, Anna Helena Reali; et al. Trajetória acadêmica da Inteligência Artificial no Brasil. In: COZMAN, Fabio G.; PLONSKI, Guilherme Ary; NERI, Hugo (org.). **Inteligência artificial: avanços e tendências**. São Paulo: Instituto de Estudos Avançados, 2021. Disponível em: <https://doi.org/10.11606/9786587773131>. Acesso em: 15 abr. 2023.

DONEDA, Danilo. Pessoa e privacidade na Sociedade da Informação. In: \_\_\_\_\_. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. Disponível em: [https://www.academia.edu/23345535/Da\\_privacidade\\_%C3%A0\\_prote%C3%A7%C3%A3o\\_de\\_dados\\_pessoais](https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais). Acesso em: 20 mar. 2023.

ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades.

**BBC News**, 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>. Acesso em: 26, dez. 2022.

EUROPEAN COMMISSION, Directorate-General for Communications Networks, Content and Technology, **Orientações éticas para uma IA de confiança**. Publications Office, 2019. Disponível em: <https://data.europa.eu/doi/10.2759/2686>. Acesso em: 22 de fev. 2023.

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional**. 9. ed. rev. ampl. e atual. Salvador. JusPODIVM, 2017. 1.728 p.

GOOGLE FOR STARTUPS; ABSTARTUPS; BOX1824. **O impacto e o futuro da Inteligência Artificial no Brasil**. 2022. Disponível em: <https://startup.google.com/intl/pt-BR/inteligencia-artificial/>. Acesso em 10 abr. 2023.

GORZONI, P. **Inteligência Artificial: Riscos para direitos humanos e possíveis ações**. 2019. Disponível em: <https://itsrio.org/wp-content/uploads/2019/03/Paula-Gorzoni.pdf>. Acesso em: 20 dez. 2022

HIGH LEVEL EXPERT GROUP ON AI. **A definition of Artificial Intelligence: main capabilities and scientific disciplines**. 2019. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Acesso em: 06 jan. 2023.

Oliveira, Ruy Flávio de. **Inteligência artificial**. Londrina: Editora e Distribuidora Educacional S.A., 2018. 224 p.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos, 1948**. Disponível em: <https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf>. Acesso em: 20 mar. 2023.

RISSE, Matthias. **Direitos Humanos e Inteligência Artificial: Uma Agenda Urgentemente Necessária**. Revista Publicum: Rio de Janeiro, v.4, n.1, 2018, p. 17-33.

SARLET, Ingo Wolfgang. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I**. Revista Consultor Jurídico: São Paulo, mar. 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protexao-dados-pessoais-direito-fundamental#autor>. Acesso em: 10 mar. 2023.

## UBERIZAÇÃO DO TRABALHO E JUVENTUDE: UMA DISCUSSÃO ACERCA DA SOCIOLOGIA DO TRABALHO

### Resumo

O presente artigo visa discutir acerca das novas metamorfoses do mundo do trabalho e suas relações de contradições com o trabalho informal, Toyotismo, terceirização, subcontratações, trabalhos temporários e as novas formas de trabalho regidas pela lógica do controle automatizado (uberização). A metodologia de análise está amparada pela Sociologia Reflexiva de Pierre Bourdieu e é feita aproximações das categorias de análise a partir dos estudos acerca da Sociologia do Trabalho desenvolvidos por Ricardo Antunes.

Palavras-chave: Mundo do Trabalho; Sociologia; Uberização.

### 1. Introdução

Para Antunes (2005), o mundo do trabalho, no capitalismo contemporâneo, vem sofrendo uma desproletarização do trabalho industrial, o que é fruto da migração do taylorismo/fordismo para o toyotismo, termo que se refere ao modelo de produção japonês desenvolvido pela Toyota entre 1948 e 1975, também conhecido como acumulação flexível. O toyotismo foi criado por Eiji Toyota (1913-

2013) e Taiichi Ohno (1912-1990), razão pela qual é também denominado ohnismo. Os principais postulados foram: just-in-time, kaizen, sistema kanban e articulação flexível. Para Antunes (2005, p. 24), é nesse momento histórico que surgem os “novos processos de trabalho... especialização flexível... vivem-se formas transitórias de produção”. A partir do toyotismo, a economia do trabalho informal se integra às rotinas modernas e produz novas relações sociais, agora pautadas na insegurança, instabilidade e inconstância.

O método de pesquisa aplicado nesse artigo foi orientado pela perspectiva praxiológica, sistêmica e relacional, fundamentadas teoricamente na Sociologia Reflexiva de Pierre Bourdieu. Entendendo que o referido método é praxiológico, pois parte-se da lógica da práxis, o que remete a uma noção da prática reflexiva da realidade e de uma crítica teórica acerca da atividade humana em sociedade; é sistêmico, pois os agentes sociais estão inseridos em um sistema que se integra e interage às mais diversas esferas da vida cotidiana; e, é relacional, pois as ações dos agentes não se dão de forma desconexa de outras instâncias formativas, sociais e históricas, e sendo assim, a compreensão da realidade

<sup>1</sup> Doutor em Educação pela PUC Goiás com estágio pós-doutoral em Educação pela UNIFAL-MG. Diretor da Escola do Futuro do estado de Goiás, unidade Luiz Rassi, em Aparecida de Goiânia.

não pode ser apreendida como fato isolado de sua própria historicidade coletiva.

A escolha dessa orientação metodológica se deu por compreender que a constituição das formulações teóricas e empíricas na construção do objeto e na investigação dos sujeitos da pesquisa, como se propõe, necessitava de uma análise de seus aspectos culturais, históricos, educacionais, sociológicos e simbólicos, no intuito de compreender as práticas, limites e tensões inerentes a uberização do trabalho.

## **2. Toyotismo, terceirização, subcontratações, uberização e trabalhos temporários**

Para Castel (1998), na modernidade, devido à diversidade empregatícia e, principalmente, à descontinuidade nas formações do trabalho, haverá um esfacelamento do emprego homogêneo e estável, sendo que esta suposta estabilidade estava presente, ainda que minimamente e precariamente, no contexto do trabalho no período da Revolução Industrial. A emergente precarização do trabalho atual aumentou a vulnerabilidade social, o que produz “no final do percurso, o desemprego e a desfiliação” (CASTEL, 1998, p. 516-517). Logo, o desemprego e a precarização do emprego se inseriram na dinâmica da modernização, premissa também partilhada por Antunes (2005), Harvey (2005a) e Bourdieu (1998).

A precariedade das relações de trabalho produz, como consequência imediata, a economia do trabalho informal. Para Demo (2003, p. 286) isto já era previsto, pois “no capitalismo nunca couberam todos os trabalhadores”. Dessa forma, no tempo presente, os trabalhadores emergem numa concorrência perversa com os próprios trabalhadores no intento de não serem demitidos, como observa Bourdieu (1998, p. 286): “A concorrência pelo trabalho é acompanhada de uma concorrência no trabalho, que é ainda uma forma de concorrência pelo trabalho, que é preciso conservar, custe o que custar, contra a chantagem da demissão”.

Segundo Garcia (2009) e Bourdieu (1997), é justamente essa flexibilidade que reestrutura o mercado a partir de bases não salariais, negando ao trabalhador a segurança e a estabilidade. Segundo Antunes (2005), o toyotismo é a resposta moderna do sistema capitalista que se adaptou à nova realidade social, pois houve uma redução na taxa de empregados nas indústrias a partir de 1980. Dessa forma, surge a subproletarização, ou seja, “trabalhadores parciais, precários, temporários, subcontratados” (ANTUNES, 2005, p. 53).

A imprevisibilidade empregatícia e os limiares do desemprego forçam, segundo Telles (2001), o surgimento de uma nova força de trabalho no cenário contemporâneo, ocupada essencialmente pelas classes pobres. Essa nova força de trabalho,

oriunda do desemprego estrutural, é chamada, pomposamente, de terceirização, subcontratações e executores de trabalhos temporários. Em alguns casos esses se autodenominam de empreendedores, ressignificando o termo e agregando novo sentido social a categoria. Entretanto, apesar da intencional criação do mito do empreendedor-desempregado, Antunes (2005, p. 49), denomina este processo de “subproletarização”, denunciando que há certa flexibilidade nas normas contratuais, permitindo que a classe paupérrima seja inserida precariamente, sem garantias e direitos, no mercado de trabalho.

Na perspectiva de Harvey (2005a), além da economia informal e do contrato flexível, o trabalhador ainda tem que conviver com o drama do desemprego. Além disso, o autor critica a intencionalidade que havia na manutenção do desemprego com fins de manter os salários dos empregados sempre baixos. Tal perspectiva, ainda que no cenário de trabalhos informais, continua tendo efeito moralizante e regulador nas classes populares.

Segundo Harvey (2005b, p. 304-305), a flexibilidade é dominada pela “ficção, pela fantasia, pelo imaterial, pelo capital fictício, pelas imagens, pela efemeridade, pelo acaso e pela flexibilidade em técnicas de produção, mercados de trabalho e nichos de consumo”. Segundo o autor, tudo isso é parte intencional de um projeto social e econômico com implicações nas relações sociais e culturais. Ser pobre e

ter um trabalho informal são, na concepção moderna, em especial no tempo presente, estados oportunos para que haja acúmulo de capital, de outrem.

### **3. A construção social e uberizada do jovem empreendedor desempregado**

A presente pesquisa se justifica, pois, no tempo presente, isto é, no cenário pós Revolução Industrial, mais especificamente a partir do final do século XX e início do século XXI, a pobreza ainda permanece atrelada ao mundo do trabalho; porém, com nova configuração nas formas de trabalho. Os trabalhadores além de terem que se submeter a salários irrisórios devido ao medo do desemprego latente e iminente, agora, também tinham que conviver com a insegurança e instabilidade do emprego. Fato esse que também não é sem intencionalidade, pois como adverte Telles (2001, p. 98),

[...] são trabalhadores que transitam entre empresas diferentes, que permanecem muito pouco tempo nos empregos que conseguem, que tem, por isso mesmo, pouca chance de se fixar em profissões ou ocupações definidas e que estão sempre, real ou virtualmente, tangenciando o mercado informal [...].

O trabalhador pobre se ajusta de forma apropriada ao modelo da acumulação flexível, pois para aqueles que se encontram na condição de pobreza qualquer opção de trabalho é tratada com uma forma de escape, ainda que temporariamente, do estereótipo de vagabundagem e criminalidade. O emprego informal promove, para a população pobre, a falsa sensação de inserção ao mundo do trabalho, dando sobrevida a falsas esperanças de ascensão social e alimentando-as.

O contexto brasileiro é marcado socialmente e historicamente por se ter uma grande parcela da sociedade que é desafortunada e que constituem suas identidades sociais a partir das relações com o mundo do trabalho. A partir dessas relações de dependência e necessidade financeira com o mundo do trabalho é que se propõe avaliar as novas formas de trabalho regidas agora pela lógica do controle automatizado (uberização), em que se reforçam as novas formas de gerenciamento algorítmico do trabalho.

O trabalho para as classes populares, segundo Renarda (2007), é entendido em termos morais, isto é, o trabalho supera o valor do salário, o que permite uma reafirmação social do trabalhador perante a comunidade local atribuindo referências simbólicas. Segundo a autora, o desemprego para os pobres é uma humilhação e uma privação moral, o que evoca a condição histórico-social da figura

do vagabundo conforme apresentada por Castel (1998) e Rizzini (1997).

Rizzini (1997) destaca que na percepção histórica da constituição do Brasil, “os pobres que se situavam mais acima na escala de moralidade eram aqueles que trabalhavam” (p. 90). A autora descreve isto se referindo ao século XX; contudo, ainda hoje, tal perspectiva permanece aplicável. Dessa forma, o trabalho para as juventudes pobres rompe a barreira econômica e agrega sentidos morais, sociais e culturais. Posto isso, o desemprego também sofre alterações na sua condição estrutural, pois a situação de desemprego, na percepção dos jovens, se traduz num impedimento de participação social efetiva e, então, assume um sentido de inadequação social.

Segundo Pais (1991), para os jovens, a condição de desempregado representa a “perda da sua identidade” (p. 974). Para o autor, o termo identidade representa as conexões das práticas sociais dos indivíduos que os tornam integrados em uma sociedade local por meio do sentimento de pertença social. Para o autor, a relação dos jovens com o mundo do trabalho pode apregoar um viés distinto do apresentado até o momento. Para ele, os jovens das classes populares encaram o trabalho de uma “forma instrumental” (p. 963). O autor explica que para os jovens “ter um qualquer trabalho é melhor do que não ter trabalho algum e um trabalho em que se ganhe mais dinheiro é melhor do

que um trabalho em que se ganha menos” (Ibidem).

Nesse cenário de ressignificação do trabalho para os jovens de classes populares, o discurso do empreendedorismo é outro aspecto importante para a compreensão das expectativas subjetivas dos jovens pobres em relação ao mundo do trabalho hodierno. Souza (2008) investiga essa relação e considera que, para os padrões do capitalismo atual, o jovem é o sujeito mais adequado para a competitividade, pois é “ajustado ao novo regime de acumulação capitalista, portador de qualidades como flexibilidade, independência, inovação. É aquele que assume riscos e busca realizar seus sonhos de ascensão e mobilidade social” (p. 160). Entretanto, na crítica de Santos (2001, p. 49), é exatamente o consumismo e a competitividade que “levam ao emagrecimento moral e intelectual da pessoa, à redução da personalidade e da visão de mundo”.

Segundo Souza (2008), a noção de jovem empreendedor é entendida pelos organismos internacionais como forma de condição protagonista, sendo o jovem, então, o principal personagem no combate à pobreza. Entretanto, tal pressuposto é uma dissimulação que produz culpabilidade unilateral nos jovens, sem levar em consideração os fatores histórico-sociais que orbitam nas histórias, limites e trajetórias que constituem os segmentos juvenis. É nessa mesma direção que se desvela o liberalismo como o princípio

motor para a concepção de que o sucesso ou o fracasso de cada indivíduo depende de si mesmo e não de uma estrutura organizacional social, por vezes externa aos próprios jovens.

O trabalho informal, ao fim, transfigura as relações de trabalho e, então, nas classes populares a luta se dá no intento de manter a condição de trabalhador, independente das condições em que se dá efetivamente o trabalho. Dessa forma, segundo a autora, a economia informal passa a ser preconizada como saudável e recomendável, como se observa no discurso dos jovens investigados. Todo esse processo endossa a lógica, segundo a qual, segundo Demo (2003, p. 286), a proposta final “não é apenas acumular riqueza, é sobretudo impedir que outros se tornem também ricos”.

A despeito das perspectivas apresentadas por Castel (1998), Harvey (2005b) e Antunes (2005), se torna notório que a figura do pobre, e suas relações sociais, vêm se modificando ao longo dos tempos, seja pelas, então, mudanças religiosas, ou governamentais, ou capitalistas, ou trabalhistas. Visto assim, o pauperismo é um estado de mutação permanente, assim como as sociedades o são. Dessa forma, as transformações histórico-sociais afetam diretamente a subjetividade da concepção de pobreza, ou seja, há diversos fatores que orbitam junto às percepções do estado de pobreza e igualmente há impressões distintas sobre

a permanência histórica do pauperismo. Contudo, admitir o fator de subjetividade intrínseco à condição da categoria pobreza, especialmente no contexto da modernidade tardia, não é admitir sua não historicidade ou não intencionalidade.

Na sociedade pós-industrializada, especialmente a partir da urbanização desarranjada, notadamente a partir do século XX, a categoria pobreza passou a ser agregada à condição humana, representando o empobrecimento dos trabalhadores, desigualdades sociais, privação material, disjunção de perspectivas de futuro e inexistência de políticas públicas efetivas. Portanto, ser pobre, nesta modernidade tardia, é se encontrar desamparado socialmente, e talvez, por esta razão, o passado, o presente e o futuro se mostram tão desconectados nas culturais juvenis, sendo que o processo de inserção dos jovens no mundo do trabalho no cenário moderno não é espontâneo e nem imparcial, mas, sim, condicionado à realidade social em que vivem.

escape, ainda que temporariamente, do estereótipo de vagabundagem e criminalidade.

O emprego informal, supostamente autônomo, promove, para a população pobre, a falsa sensação de inserção ao mundo do trabalho, dando sobrevida a falsas esperanças de ascensão social, que por vezes se limitam ao trabalho informal, terceirizado, com subcontratações, trabalhos temporários e as novas formas de trabalho condicionados a lógica do controle automatizado (uberização).

#### 4. Considerações finais

O trabalhador, e talvez mais especificamente o trabalhador jovem pobre, se ajusta de forma apropriada ao modelo da acumulação flexível e as novas formas de uberização do trabalho. Isso se deve ao fato de que para aqueles que se encontram na condição de pobreza qualquer opção de trabalho é tratada com uma forma de

## Referências

ANTUNES, Ricardo. **Adeus ao trabalho?** Ensaio sobre as metamorfoses e centralidade do mundo do trabalho. 10ª ed. São Paulo: Cortez, 2005.

BOURDIEU, Pierre et al. **A miséria do mundo**. Petrópolis, RJ: 1997

BOURDIEU, Pierre. **Contrafogos**: táticas para enfrentar a invasão neoliberal. Rio de Janeiro: Zahar, 1998.

CASTEL, Robert. **As metamorfoses da questão social**: uma crônica do salário. Petrópolis: Vozes, 1998.

DEMO, Pedro. **Pobreza da pobreza**. Petrópolis, RJ: Vozes: 2003.

GARCIA, Dirce Maria Falcone. **Juventude em tempo de incertezas**: enfrentando desafios na educação e no trabalho. São Paulo: Annablume, 2009.

HARVEY, David. **A produção capitalista do espaço**. São Paulo: Annablume, 2005a.

HARVEY, David. **Condição pós-moderna**. São Paulo: Loyola, 2005b.

PAIS, José Machado. Emprego juvenil e mudança social: velhas teses, novos modos de vida. **Revista Análise Social**. Universidade de Lisboa, Lisboa, v. XXVI, n. 114, pp. 945-987. 1991.

RENARDA, Ava. **O caráter multifacetado da pobreza**: a relação entre concepção e intervenção. 2007. 162 f. Dissertação (Mestrado em Política Social) - Universidade Federal do Espírito Santo, Vitória, 2007.

RIZZINI, Irene. **O século perdido**: raízes históricas das políticas públicas para a infância no Brasil. Rio de Janeiro: Editora Universitária Santa Úrsula, 1997.

SANTOS, Milton. **Por uma outra globalização**: do pensamento único à consciência universal. 6 ed. Rio de Janeiro: Record, 2001.

SOUZA, Adriano Mohn. O discurso do empreendedorismo para jovens trabalhadores. In: GUIMARÃES, Maria Tereza Canezin (org.). **Estudos sobre jovens e processos educativos na contemporaneidade**. Goiânia: Editora da UCG, 2008.

TELLES, Vera da Silva. **Pobreza e Cidadania**. São Paulo: USP, 2001.