

Inteligência Artificial e Segurança Pública: Modelo Integrado com ODS e RRI

Artificial Intelligence in Public Security: An Integrated Governance Model Aligned with SDGs and RRI

Emmanuel Bohrer Junior – Universidade Federal de Santa Catarina (UFSC) -
bohrer2303@yahoo.com.br

RESUMO:

Este artigo apresenta um estudo sobre o uso da Inteligência Artificial (IA) na Segurança Pública, destacando seus potenciais impactos sociais, desafios éticos e contribuições para o desenvolvimento sustentável. O objetivo central é propor um modelo integrado de governança responsável que alinhe as aplicações de IA – como análise preditiva de crimes, monitoramento inteligente e auditoria algorítmica – aos Objetivos de Desenvolvimento Sustentável (ODS), com ênfase nos ODS 9, 10, 11 e 16, e aos princípios de *Responsible Research and Innovation* (RRI). A pesquisa adota uma abordagem qualitativa e exploratória, estruturada em quatro etapas: revisão bibliográfica sistemática (2018–2025), mapeamento de experiências internacionais, identificação de riscos éticos (viés, privacidade e discriminação automatizada) e desenvolvimento de um framework conceitual para orientar políticas públicas. O modelo proposto é composto por quatro eixos estratégicos: governança transparente, auditoria algorítmica, alinhamento com os ODS e capacitação contínua de profissionais. Os resultados esperados incluem maior transparência institucional, mitigação de vieses, fortalecimento da confiança pública, integração da IA às metas de desenvolvimento sustentável e promoção de uma governança tecnológica mais inclusiva e responsável. Este estudo contribui para a construção de políticas públicas que conciliem inovação tecnológica, direitos fundamentais e justiça social no contexto da Segurança Pública.

Palavras-chave: 1. Inteligência Artificial 2. Segurança Pública 3. Governança Responsável 4. Desenvolvimento Sustentável 5. Auditoria Algorítmica.

ABSTRACT:

This article presents a study on the use of Artificial Intelligence (AI) in Public Security, highlighting its potential social impacts, ethical challenges, and contributions to sustainable development. The central objective is to propose an integrated model of responsible governance that aligns AI applications—such as crime predictive analysis, intelligent monitoring, and algorithmic auditing—with the Sustainable Development

Goals (SDGs), with emphasis on SDGs 9, 10, 11, and 16, and the principles of Responsible Research and Innovation (RRI). The research adopts a qualitative and exploratory approach, structured in four stages: systematic literature review (2018–2025), mapping of international experiences, identification of ethical risks (bias, privacy, and automated discrimination), and development of a conceptual framework to guide public policies. The proposed model is composed of four strategic pillars: transparent governance, algorithmic auditing, alignment with the SDGs, and continuous training of professionals. The expected results include greater institutional transparency, mitigation of biases, strengthening of public trust, integration of AI into sustainable development goals, and promotion of more inclusive and responsible technological governance. This study contributes to the construction of public policies that reconcile technological innovation, fundamental rights, and social justice in the context of Public Security.

Keywords: 1. Artificial Intelligence 2. Public Security 3. Responsible Governance 4. Sustainable Development 5. Algorithmic Auditing.

1 INTRODUÇÃO

A aplicação da Inteligência Artificial (IA) em Segurança Pública representa uma das mais significativas transformações tecnológicas do século XXI. Ferramentas de IA têm sido empregadas para análise preditiva de crimes, reconhecimento de padrões comportamentais, monitoramento urbano e otimização de recursos policiais.

Segundo Russell e Norvig (2010), a IA é definida como o estudo de agentes que percebem seu ambiente e tomam decisões para maximizar suas chances de sucesso. No contexto da segurança pública, isso se traduz em sistemas capazes de identificar padrões criminais, prever ocorrências e auxiliar na tomada de decisões estratégicas.

Contudo, essas inovações também trazem riscos associados à privacidade, ao viés algorítmico e à desconfiança social. De acordo com Zuboff (2019), a vigilância digital pode comprometer direitos fundamentais se não for regulada por princípios éticos e legais. A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709/2018, estabelece diretrizes para o tratamento de dados pessoais, sendo essencial para a implementação de sistemas de IA que respeitem os direitos dos cidadãos (BRASIL, 2018).

A crescente digitalização das atividades humanas tem impulsionado o uso de tecnologias avançadas, como a IA, em diversos setores, incluindo a Segurança Pública. A IA oferece ferramentas poderosas para análise de dados, reconhecimento de padrões

e tomada de decisão automatizada, que podem transformar a forma como as instituições de segurança operam. Segundo Floridi et al. (2018), a IA deve ser desenvolvida e aplicada com base em princípios éticos que garantam sua contribuição para uma sociedade justa e equitativa.

O presente estudo tem como objetivo propor um modelo conceitual de governança responsável para o uso da IA na Segurança Pública, integrando os 17 Objetivos de Desenvolvimento Sustentável (ODS) da ONU e os princípios de *Responsible Research and Innovation* (RRI).

Ao alinhar tecnologia e ética, busca-se contribuir para políticas públicas mais eficazes, transparentes e socialmente justas. A proposta visa promover a transparência, a inclusão social e a eficiência institucional, contribuindo para o fortalecimento da confiança pública nas tecnologias emergentes.

Como destaca Van den Hoven (2014), a inovação responsável requer antecipação dos impactos, participação dos atores sociais e reflexividade nos processos decisórios.

Este artigo propõe um modelo integrado de governança tecnológica que combina os Objetivos de Desenvolvimento Sustentável (ODS) da ONU com os princípios de Responsible Research and Innovation (RRI), visando orientar a aplicação ética e eficaz da IA na Segurança Pública.

2. FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica deste estudo parte da intersecção entre tecnologia, ética e políticas públicas, com foco na aplicação da Inteligência Artificial (IA) na Segurança Pública. A IA, definida por Russell e Norvig (2010) como sistemas capazes de perceber o ambiente e tomar decisões para atingir objetivos, tem sido amplamente utilizada em contextos de segurança para análise preditiva, reconhecimento facial e gestão de dados operacionais.

2.1 Inteligência Artificial na Segurança Pública

A Inteligência Artificial (IA) tem sido amplamente aplicada na Segurança Pública, com destaque para sistemas de vigilância inteligente, análise preditiva de crimes e gestão de recursos operacionais.

Segundo Floridi et al. (2018), a IA deve ser desenvolvida com base em princípios éticos que garantam sua contribuição para uma sociedade justa e equitativa. No contexto da segurança, algoritmos de aprendizado de máquina são utilizados para identificar padrões comportamentais e prever ocorrências criminais, permitindo uma atuação mais eficiente das forças policiais. No entanto, o uso indiscriminado dessas tecnologias pode reforçar preconceitos e ampliar desigualdades sociais (OECD, 2019).

2.2 Objetivos de Desenvolvimento Sustentável (ODS)

Os ODS da ONU fornecem um marco global para o desenvolvimento sustentável, sendo fundamentais para orientar políticas públicas que envolvem tecnologias emergentes. O ODS 16 trata de paz, justiça e instituições eficazes, diretamente relacionado à Segurança Pública. O ODS 9 incentiva a inovação e infraestrutura resiliente, enquanto o ODS 10 busca reduzir desigualdades e o ODS 11 promove cidades sustentáveis (UNITED NATIONS, 2015). A integração desses objetivos com a aplicação da IA permite alinhar inovação tecnológica com justiça social e sustentabilidade urbana.

2.2.1 Objetivos de Desenvolvimento Sustentável (ODS) e sua Relação com a IA na Segurança Pública

ODS 9 – Indústria, Inovação e Infraestrutura - Os Objetivos de Desenvolvimento Sustentável (ODS) da ONU fornecem um marco global para o desenvolvimento sustentável, sendo fundamentais para orientar políticas públicas que envolvem tecnologias emergentes. A integração desses objetivos com a aplicação da Inteligência

Artificial (IA) permite alinhar inovação tecnológica com justiça social e sustentabilidade urbana.

ODS 10 – Redução das Desigualdades - Este objetivo busca reduzir as desigualdades dentro dos países e entre eles. A aplicação da IA na Segurança Pública pode tanto mitigar quanto exacerbar desigualdades sociais, dependendo de como os algoritmos são desenvolvidos e utilizados. Estudos mostram que sistemas de IA treinados com dados enviesados podem reproduzir discriminações históricas, afetando desproporcionalmente grupos vulneráveis (OECD, 2019). Para que a IA contribua para a redução das desigualdades, é essencial implementar mecanismos de auditoria algorítmica, garantir a representatividade nos dados e promover a inclusão digital.

ODS 11 – Cidades e Comunidades Sustentáveis - O ODS 11 propõe tornar as cidades e comunidades inclusivas, seguras, resilientes e sustentáveis. A IA pode desempenhar um papel estratégico na gestão urbana inteligente, por meio de sistemas de vigilância, análise de tráfego, monitoramento ambiental e prevenção de crimes. Tecnologias como câmeras inteligentes e sensores conectados a redes neurais podem melhorar a segurança em espaços públicos, desde que respeitem os direitos à privacidade e à liberdade. A integração da IA com políticas urbanas deve ser feita com transparência e participação social, garantindo que os benefícios da tecnologia sejam distribuídos equitativamente (Floridi et al., 2018).

ODS 16 – Paz, Justiça e Instituições Eficazes - Este objetivo busca promover sociedades pacíficas e inclusivas, garantir o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas. A IA pode fortalecer a capacidade institucional por meio da automação de processos judiciais, análise de dados criminais e apoio à tomada de decisão estratégica. No entanto, sem uma governança robusta, essas tecnologias podem comprometer direitos fundamentais e gerar desconfiança social. Van den Hoven (2014) argumenta que a inovação responsável deve ser guiada por valores democráticos, com participação ativa da sociedade civil.

2.3 Princípios de Responsible Research and Innovation (RRI)

A abordagem de RRI propõe que a pesquisa e inovação sejam conduzidas com responsabilidade, antecipando impactos, promovendo inclusão e garantindo transparência. Van den Hoven (2014) destaca que a RRI deve envolver todos os atores sociais no processo de inovação, incluindo pesquisadores, formuladores de políticas e cidadãos. Os princípios de RRI incluem antecipação, inclusão, transparência, responsabilidade e reflexividade, sendo essenciais para orientar o desenvolvimento ético da IA na Segurança Pública.

2.4 Governança Tecnológica

A governança tecnológica refere-se à criação de mecanismos institucionais que regulam o desenvolvimento e uso de tecnologias. Modelos eficazes de governança devem incluir auditoria algorítmica, participação social e capacitação contínua dos profissionais envolvidos. Segundo Floridi et al. (2018), a governança deve ser orientada por valores democráticos e direitos humanos, garantindo que as tecnologias emergentes sejam utilizadas de forma ética e responsável. No contexto da Segurança Pública, a governança tecnológica é essencial para mitigar riscos como o viés algorítmico e a violação da privacidade.

3. METODOLOGIA

A pesquisa adotou uma abordagem qualitativa e exploratória, com foco na construção de um modelo conceitual de governança responsável para o uso da Inteligência Artificial (IA) na Segurança Pública. Segundo Minayo (2001), a pesquisa qualitativa é adequada para compreender fenômenos complexos e contextuais, como o impacto da tecnologia nas políticas públicas.

O estudo foi estruturado em quatro etapas principais:

1. Revisão bibliográfica sistemática sobre aplicações de IA na Segurança Pública, com foco em publicações entre 2018 e 2025, utilizando bases como *Scopus*, *Web of Science* e *SciELO*;

2. Mapeamento de experiências internacionais de governança de IA em países como Reino Unido, Canadá, Alemanha e Estônia, com análise documental de políticas públicas e relatórios técnicos;

3. Identificação dos principais riscos éticos associados à IA, como viés algorítmico, invasão de privacidade, uso indevido de dados e discriminação automatizada, conforme discutido por Floridi et al. (2018) e OECD (2019);

4. Construção de um modelo conceitual baseado nos Objetivos de Desenvolvimento Sustentável (ODS) da ONU e nos princípios de Responsible Research and Innovation (RRI), conforme Van den Hoven (2014).

A análise dos dados foi conduzida por meio de análise temática, conforme Braun e Clarke (2006), permitindo a identificação de padrões conceituais recorrentes na literatura e nos documentos normativos. A triangulação de fontes foi utilizada para aumentar a validade dos achados, combinando dados teóricos, empíricos e normativos. Na análise se procurou verificar os principais riscos éticos (viés, privacidade e uso indevido), bem como na análise dos dados seguiu o método de análise temática, priorizando conceitos recorrentes em literatura científica e documentos normativos.

4. DESENVOLVIMENTO E RESULTADOS

O modelo conceitual proposto neste estudo é estruturado em quatro eixos estratégicos que visam orientar a aplicação ética, eficaz e sustentável da IA na Segurança Pública. Cada eixo foi desenvolvido com base em evidências empíricas e referenciais teóricos, conforme descrito a seguir:

4.1. Governança Transparente:

Este eixo propõe a criação de comitês interinstitucionais com participação da sociedade civil, especialistas em tecnologia, representantes do sistema de justiça e organizações de direitos humanos. A transparência é essencial para garantir a legitimidade das decisões tecnológicas, conforme destaca Van den Hoven (2014).

Experiências como o *Ethics Advisory Board* do Reino Unido demonstram que a inclusão social na governança tecnológica aumenta a confiança pública.

4.2. Auditoria Algorítmica:

A auditoria de algoritmos é fundamental para detectar e mitigar vieses discriminatórios. Ferramentas como *FairML* e *AI Fairness 360* têm sido utilizadas para avaliar a equidade de sistemas de IA. Segundo Floridi et al. (2018), a auditoria deve ser contínua e envolver especialistas multidisciplinares. No Brasil, a LGPD (BRASIL, 2018) estabelece princípios de responsabilização e prestação de contas que sustentam essa prática.

4.3. Alinhamento com ODS:

Este eixo propõe o uso de indicadores sociais e ambientais para avaliar o impacto da IA na Segurança Pública. Por exemplo, o ODS 16 pode ser monitorado por meio de métricas de redução da violência e aumento da confiança institucional. O ODS 10 pode ser avaliado por meio da equidade no tratamento de diferentes grupos sociais. A integração dos ODS permite que a inovação tecnológica seja orientada por metas de justiça social e sustentabilidade (UNITED NATIONS, 2015).

4.4. Capacitação Contínua:

A formação de profissionais de segurança em ética digital, proteção de dados e fundamentos de IA é essencial para garantir o uso responsável da tecnologia. Programas de capacitação devem incluir oficinas, cursos de extensão e certificações. Segundo OECD (2019), a capacitação contínua é um dos pilares para a implementação eficaz de tecnologias emergentes no setor público.

Os resultados esperados com a aplicação do modelo incluem maior transparência institucional, redução de vieses algorítmicos, alinhamento das políticas de segurança com os ODS e fortalecimento da confiança pública.

A Figura 1 ilustra o modelo de governança integrada, conectando os quatro eixos estratégicos com os princípios de RRI e os ODS.

Figura 1 - Modelo Integrado de Governança para IA na Segurança Pública



Fonte: desenvolvido pelo autor, 2025.

Este modelo integrado sintetiza o modelo conceitual proposto para a governança da Inteligência Artificial na Segurança Pública, integrando os eixos estratégicos, os Objetivos de Desenvolvimento Sustentável (ODS) relevantes e os princípios de Responsible Research and Innovation (RRI).

Núcleo central:

Tecnologia de IA aplicada à Segurança Pública: análise preditiva de crimes, monitoramento inteligente, gestão automatizada de processos e auditoria de viés.

Quatro eixos estratégicos:

1. Governança Transparente: comitês interinstitucionais, participação da sociedade civil e políticas abertas.
2. Auditoria Algorítmica: ferramentas de explicabilidade, mitigação de vieses e responsabilização.
3. Alinhamento com ODS: ODS 9, 10, 11 e 16 com indicadores sociais e ambientais.
4. Capacitação Contínua: formação em ética digital, educação em IA e certificação periódica.

Camada externa (valores e princípios):

- Ética, Transparência, Inclusão, Responsabilidade, Reflexividade.

SUSTENTAÇÃO:

- Princípios de RRI (antecipação, inclusão, reflexividade, ética, participação).
- LGPD e legislação nacional como base normativa.

Resultados esperados:

- Redução de vieses, aumento da transparência institucional, fortalecimento da confiança pública e integração efetiva dos ODS

5. DISCUSSÃO

A discussão sobre o uso da Inteligência Artificial (IA) na Segurança Pública exige uma análise crítica dos impactos sociais, éticos e institucionais. Experiências internacionais demonstram que a adoção de IA sem mecanismos de governança pode gerar efeitos adversos, como discriminação algorítmica e perda de confiança pública. No Reino Unido, por exemplo, o uso de sistemas de reconhecimento facial pela polícia foi alvo de críticas por falta de transparência e por resultados enviesados (FLORIDI et al., 2018). Já no Canadá, iniciativas de auditoria algorítmica e participação cidadã têm promovido maior legitimidade no uso dessas tecnologias (OECD, 2019).

No Brasil, o desafio é ainda maior devido às desigualdades estruturais e à fragilidade institucional. A Lei Geral de Proteção de Dados (LGPD) representa um avanço importante, mas sua aplicação na Segurança Pública requer regulamentações específicas e capacitação dos agentes envolvidos (BRASIL, 2018). A integração dos Objetivos de Desenvolvimento Sustentável (ODS) e dos princípios de Responsible Research and Innovation (RRI) pode oferecer um caminho para a construção de políticas públicas mais justas e eficazes. Van den Hoven (2014) destaca que a inovação responsável deve ser orientada por valores democráticos e envolver todos os atores sociais no processo decisório.

Experiências em países como Reino Unido e Canadá indicam que a adoção de IA em Segurança Pública sem transparência pode resultar em descrédito institucional e aumento das desigualdades. Por outro lado, iniciativas que integram princípios de RRI e alinhamento com os ODS demonstram maior aceitação social e eficácia a longo prazo.

O Brasil tem uma oportunidade estratégica de se posicionar como referência em inovação responsável neste setor, considerando sua legislação de proteção de dados (LGPD) e iniciativas de transformação digital.

Como explanado anteriormente de forma mais ampla, o modelo proposto é composto por quatro eixos estratégicos:

1. Governança Transparente: Envolve a criação de comitês interinstitucionais com participação da sociedade civil, garantindo que as decisões sobre o uso da IA sejam tomadas de forma democrática e inclusiva.

2. Auditoria Algorítmica: Consiste na implementação de ferramentas para detectar e mitigar vieses nos sistemas de IA. A auditoria deve ser contínua e envolver especialistas independentes.

3. Alinhamento com ODS: Estabelece indicadores de impacto social e ambiental para avaliar a contribuição das tecnologias para o desenvolvimento sustentável.

4. Capacitação Contínua: Propõe programas de formação para profissionais de segurança, abordando temas como ética digital, proteção de dados e uso responsável da IA.

Os resultados indicam que a adoção de um modelo integrado pode aumentar a eficácia das políticas públicas, reduzir desigualdades e fortalecer a confiança institucional.

Quadro 1 – Relação entre Aplicações de IA, ODS e RRI

APLICAÇÃO DE IA	ODS RELACIONADOS	IMPACTOS ESPERADOS	PRINCÍPIOS RRI
Análise preditiva de crimes	ODS 16	Redução de criminalidade e uso estratégico de recursos	Antecipação, Ética
Monitoramento inteligente	ODS 11	Aprimoramento da prevenção em áreas urbanas	Transparência, Inclusão
Gestão automatizada de processos	ODS 9	Eficiência em investigações e processos judiciais	Responsabilidade, Participação
Auditoria de viés	ODS 10	Minimização de discriminações e injustiças	Reflexividade, Ética

Fonte: Elaborado pelo autor, 2025.

6 IMPACTOS PARA A SOCIEDADE

A implementação do modelo de governança para a Inteligência Artificial (IA) na Segurança Pública tem o potencial de gerar transformações estruturais significativas no relacionamento entre tecnologia, instituições e cidadãos. Ao integrar os quatro eixos estratégicos – Governança Transparente, Auditoria Algorítmica, Alinhamento com os ODS e Capacitação Contínua – com os princípios de Responsible Research and

Innovation (RRI), é possível estabelecer um ecossistema tecnológico que privilegie justiça social, equidade e confiança pública.

6. 1. Fortalecimento da Transparência Institucional

A criação de comitês interinstitucionais e a adoção de políticas abertas garantem maior legitimidade social das decisões tecnológicas, reduzindo a assimetria de informações entre Estado e cidadãos. Isso favorece a construção de uma cultura de confiança pública, essencial para a aceitação da IA em processos de segurança.

6. 2. Redução de Vieses e Discriminações

A auditoria algorítmica, quando aplicada de forma contínua e independente, contribui para a mitigação de discriminações históricas, evitando que sistemas de IA reproduzam preconceitos estruturais. Tal prática reforça os direitos fundamentais previstos na LGPD e promove a equidade no tratamento de diferentes grupos sociais.

6. 3. Alinhamento com Objetivos de Desenvolvimento Sustentável (ODS)

O modelo proposto promove impactos positivos sobre:

ODS 9: fortalecendo a inovação e a infraestrutura digital no setor público;

ODS 10: reduzindo desigualdades sociais por meio de decisões mais justas e baseadas em dados éticos;

ODS 11: contribuindo para cidades mais seguras e resilientes;

ODS 16: aprimorando a eficácia institucional e o acesso à justiça.

6.4. Empoderamento e Educação Digital

A capacitação contínua de agentes de segurança, associada à inclusão da sociedade civil nos processos decisórios, resulta em maior alfabetização digital e no

fortalecimento da cidadania ativa. A formação em ética digital e fundamentos de IA previne o uso indevido da tecnologia e amplia as oportunidades de participação social.

6.5. Sustentação Ética e legal

O modelo conceitual ancora-se em princípios como ética, transparência, inclusão, responsabilidade e reflexividade, articulados com a legislação nacional (LGPD) e padrões internacionais de inovação responsável. Essa sustentação garante que a evolução tecnológica ocorra dentro de parâmetros democráticos e com proteção efetiva aos direitos dos cidadãos.

6.6 Impacto Global

A adoção desse modelo gera efeitos sistêmicos: aumento da eficiência operacional das instituições de segurança, redução do déficit de confiança entre sociedade e Estado, e promoção de uma governança tecnológica mais justa e sustentável, conectando a inovação digital às demandas sociais e aos compromissos internacionais assumidos pelo Brasil.

7. CONSIDERAÇÕES FINAIS

Conclui-se que a aplicação da Inteligência Artificial na Segurança Pública deve ser conduzida com responsabilidade, transparência e alinhamento aos valores democráticos. O modelo conceitual proposto neste estudo, baseado nos ODS e nos princípios de RRI, oferece uma estrutura para orientar gestores públicos na implementação ética e eficaz de tecnologias emergentes. A governança tecnológica, quando bem estruturada, pode mitigar riscos como o viés algorítmico e a violação da privacidade, ao mesmo tempo em que potencializa a eficiência institucional.

Recomenda-se que futuras políticas públicas incorporem mecanismos de auditoria algorítmica, promovam a capacitação contínua dos profissionais de segurança e incentivem a participação social nos processos decisórios. Além disso, é fundamental que sejam realizados estudos empíricos para avaliar os impactos reais da IA na Segurança Pública brasileira, considerando as especificidades regionais e culturais. A

construção de um observatório nacional de IA e Segurança Pública pode ser um passo estratégico para monitorar, avaliar e aprimorar continuamente essas iniciativas.

A Inteligência Artificial pode potencializar a Segurança Pública, mas somente quando utilizada de forma ética, transparente e alinhada aos objetivos sociais. O modelo proposto neste artigo contribui para a construção de políticas mais robustas, orientando a integração entre tecnologia e cidadania.

Como próximos passos, recomenda-se a implementação piloto em delegacias-modelo, a realização de consultas públicas e a criação de um observatório nacional para monitoramento contínuo dos impactos da IA na Segurança.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRAUN, Virginia; CLARKE, Victoria. **Using thematic analysis in psychology**. *Qualitative Research in Psychology*, v. 3, n. 2, p. 77–101, 2006.

FLORIDI, Luciano et al. AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. **Minds and Machines**, v. 28, p. 689–707, 2018.

MINAYO, Maria Cecília de Souza. **O desafio do conhecimento: pesquisa qualitativa em saúde**. 9. ed. São Paulo: Hucitec, 2001.

OECD. **Artificial Intelligence in Society**. Paris: OECD Publishing, 2019.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. 3. ed. Upper Saddle River: **Prentice Hall**, 2010.

UNITED NATIONS. **Transforming our world: the 2030 Agenda for Sustainable Development**. New York: UN, 2015.

VAN DEN HOVEN, Jeroen. **Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society**. Chichester: Wiley, 2014.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019