10.37334/ricts.v8i2.164

A BIOMETRIA COMO PRETEXTO DE FALÊNCIA GLOBAL DA INTERNET – A SOCIEDADE BÁRBARA[1]

Biometrics as a pretext for the global failure of the internet – The barbaric society

COSTA, Joniválnio Cassuada da[2]; & KIMBANDA, Francisco Jacucha Cahuco[3]

Resumo

Ora bem, este artigo discute a biometria como dispositivo de controle social e político, apontando como sua imposição crescente pode atuar como catalisador de um colapso das estruturas globais da internet. Argumenta-se, portanto, que a biometria, sob a justificativa de segurança e eficiência, revela-se um pretexto para vigilância massiva, exclusão digital e erosão de direitos fundamentais, conduzindo a um estado de "barbárie tecnológica". Portanto, esste artigo propõe objetivamente que a biometria constitua não apenas ferramenta de identificação, mas, sobretudo pretexto para legitimar a falência do projeto emancipatório da internet. O artigo fundamenta-se em referenciais críticos da sociologia, filosofia política e estudos de tecnologia.

Abstract

Well than, this article discusses biometrics as a device of social and political control, highlighting how its increasing imposition can act as a catalyst for a collapse of global internet structures. It argues, therefore, that biometrics, under the guise of security and efficiency, proves to be a pretext for mass surveillance, digital exclusion, and the erosion of fundamental rights, leading to a state of "technological barbarism". Therefore, this article objectively proposes that biometrics constitute not only an identification tool but, above all, a pretext to legitimize the failure of the internet's emancipatory project. The article is grounded in critical frameworks from sociology, political philosophy, and technology studies.

Palavras-chave: *Biometria; Internet; Vigilância; Barbárie; Exclusão digital.*

Keywords: *Biometrics; Internet; Surveillance; Barbarism; Digital exclusion.*

Data de submissão: outubro 2025 | **Data de publicação**: dezembro 2025.

[1] Artigo padronizado, formatado, colocado no template e indexado pela equipa de voluntários da MUNDIS – Associação Cívica de Formação e Cultura: https://www.mundiseventos.pt/.

[2] JONIVÁNIO CASSUADA DA COSTA - Universidade Rainha Njinga A Mbandi & Analista Político e Comentador do Programa Conversas Africanas da Emissora da Rádio Provincial de Malanje ANGOLA. Email: jonivaniocassuada@gmail.com

[3] FRANCISCO JACUCHA CAHUCO KIMBANDA - Universidade Agostinho Neto, ANGOLA. Email: francisco.jacucha1@uan.ao

> "Não devemos nos fixar no que esse novo arsenal de tecnologias digitais nos permite fazer sem antes perguntar o que realmente vale a pena ser feito" Evgeny Morozov.

INTRODUÇÃO

Partimos do pressuposto de que a internet, enquanto espaço global de comunicação, foi concebida como instrumento de partilha e democratização do conhecimento. No entanto, sua crescente captura por mecanismos de vigilância estatal e corporativa transforma-a em espaço de controle. A biometria emerge como dispositivo central nesse processo: impressões digitais, reconhecimento facial, íris e voz tornaram-se chaves obrigatórias de acesso.

O ponto decisivo está em que esses sistemas não são apenas meios de autenticação, mas portas de entrada para a captura de dados íntimos do corpo humano. Ao exigir biometria para acessar serviços digitais, governos e corporações passam a deter não apenas informações cadastrais, mas traços biológicos únicos e irreversíveis. Isso significa que a identidade digital deixa de ser um simples código de acesso e passa a ser uma extensão inseparável do corpo, submetida à lógica do mercado e da vigilância (Zuboff, 2019).

Na mesma linha de pensamento, Bruce Schneier (2015) é direto ao afirmar que a coleta biométrica representa a fase mais avançada do modelo de negócio da internet baseado na vigilância, pois o usuário não tem opção: "ou aceita entregar seus dados, ou fica excluído". Nesse sentido, a biometria opera como mecanismo de coerção disfarçado de conveniência tecnológica. Defende-se, portanto, que a biometria atua como pretexto político e ideológico[4] para a erosão do projeto emancipatório da internet, legitimando exclusões e hierarquizações digitais.

[4] A biometria, assim, não é escolha livre, mas imposição silenciosa que redefine a cidadania digital a partir da submissão ao código algorítmico. Essa apropriação técnica projeta-se como forma de barbárie contemporânea. Diferente da ideia clássica do bárbaro como ausência de civilização, aqui se trata do excesso instrumental da técnica que subjuga a dignidade humana. Fanon (1961/2005) já denunciava a violência das estruturas classificatórias coloniais que reduziam sujeitos à condição de objetos. Hoje, a lógica biométrica repete essa violência no espaço digital: quem não é reconhecido pelo algoritmo torna-se inexistente para o sistema.

A análise insere-se no debate crítico acerca da vigilância, da colonialidade e da modernidade tecnológica, problematizando como a promessa de segurança e eficiência encobre a consolidação de uma nova forma de barbárie informacional.

Ora bem, a situação é gravíssima, é embaraçosa e lastimável, pois, esse quadro, infelizmente, coloca em causa os Direitos Humanos e Fundamentais consagrados pela Declaração Universal dos Direitos Humanos (ONU, 1948). Nos termos do artigo 1º afirma que "todos os seres humanos nascem livres e iguais em dignidade e em direitos", mas a imposição da biometria estabelece uma hierarquia de reconhecimento que exclui os não identificados digitalmente. Além disso, o artigo 12º garante que "ninguém será sujeito a interferências arbitrárias em sua vida privada", o que é diretamente violado pela coleta compulsória de dados biométricos. Logo, a expansão do controle digital implica um paradoxo: em nome da segurança, compromete-se a própria base da dignidade humana.

Então, a biometria opera como pretexto político e ideológico para a erosão do projeto emancipatório da internet, legitimando exclusões e hierarquizações digitais. O que deveria ser espaço de circulação livre de saberes converte-se em um ambiente marcado pela vigilância, pela segmentação e pela negação de humanidade. A análise que segue insere-se nesse debate crítico, discutindo como a promessa de segurança e eficiência oculta a consolidação de uma sociedade bárbara informacional, onde a tecnologia não emancipa, mas oprime, em clara contradição com os princípios fundadores da Carta da ONU. É de facto aqui onde reside a problemática deste artigo; é justamente isso a que denominamos por sociedade bárbara.

Nessa ordem de ideias, o problema de pesquisa é:

Será que a utilização da biometria como requisito de acesso digital compromete os direitos humanos e fundamentais consagrados pela Carta da ONU, transformando a internet de um espaço emancipatório em uma sociedade bárbara informacional?

Para o efeito, eis as hipóteses:

1. *Hipótese principal:* A biometria, embora apresentada como instrumento de segurança digital, funciona como dispositivo político e ideológico que reforça mecanismos de exclusão, violando princípios fundamentais da dignidade humana.

2. *Hipótese secundária 1:* A exigência de credenciais biométricas constitui um processo de hierarquização digital que contradiz o princípio de igualdade universal estabelecido pela Declaração Universal dos Direitos Humanos.
3. *Hipótese secundária 2:* A biometria legitima a consolidação de um modelo de internet fragmentada, controlada por Estados e corporações, caracterizando um processo de regressão civilizatória que pode ser descrito como barbárie tecnológica.

Portanto, para responder o problema levantado e auxiliar as hipóteses, elaboramos os seguintes objectivos:

Objetivo geral:

Analisar criticamente o uso da biometria como pretexto de controle digital e discutir como este processo conduz à violação de direitos humanos fundamentais, contribuindo para a constituição de uma sociedade bárbara informacional.

Objetivos específicos:

- Examinar o papel da biometria na arquitetura de vigilância digital contemporânea.
- Correlacionar a coleta compulsória de dados biométricos com os princípios da Declaração Universal dos Direitos Humanos.
- Identificar os impactos da biometria na exclusão digital e na produção de hierarquizações sociais.
- Investigar como autores da sociologia crítica e da teoria tecnológica interpretam os riscos do controle algorítmico.
- Argumentar que a utilização da biometria, em vez de proteger, pode induzir a uma forma de barbárie digital legitimada.

Daí que, este artigo justifica-se pela necessidade de problematizar criticamente a utilização da biometria na era digital. Embora apresentada como solução técnica para a segurança, tal prática implica consequências sociais, políticas e éticas que não podem ser ignoradas. A captura de dados corporais inalienáveis transforma a identidade humana em objeto de mercado e de vigilância permanente, colocando em risco direitos fundamentais como a privacidade, a liberdade e a igualdade.

Vale a pena dizer que, o tema reveste-se de relevância teórica e prática. Do ponto de vista académico, contribui para a reflexão interdisciplinar entre tecnologia, sociologia e direitos humanos. Do ponto de vista social, alerta para os perigos da naturalização da vigilância biométrica, em especial nos países do Sul global e países africanos onde a ausência de regulações adequadas agrava as vulnerabilidades. Ao correlacionar o avanço tecnológico com a noção de barbárie, o artigo busca evidenciar que o problema não está na tecnologia em si, mas no modo como ela é apropriada para fins de exclusão e controle, em contradição direta com os princípios fundadores da ONU. Portanto, investigar a biometria como pretexto de falência global da internet significa questionar o próprio futuro da cidadania digital e da dignidade humana no século XXI (o marco **teórico** deste artigo tem como base em Castells, Morozov, Diop e Fanon, integrando esses pontos de vigilância, colonialidade e barbárie digital).

ENQUADRAMENTO TEÓRICO

A teoria da sociedade em rede

Se olharmos para a teoria de Manuel Castells (1999) vamos verificar que a internet representa o núcleo organizador da sociedade em rede, constituindo-se como uma infraestrutura comunicacional que redefine as relações de poder, identidade e produção. Para o autor, a conectividade não é neutra: ela depende de quem controla os fluxos informacionais e os códigos que estruturam a rede (Castells, 1999, p. 23). Ao situar a biometria nesse contexto, observa-se que ela se torna uma tecnologia de "nó" e "fluxo" — um ponto de passagem obrigatória que filtra, permite ou nega acesso. Assim, o ideal de democratização da rede é tensionado pela captura dos corpos como senha de entrada, gerando uma arquitetura de exclusão.

A colonialidade da técnica

No viés do pensador africano, a ciência e a técnica, ao longo da história, não são neutras, mas instrumentos de hegemonia cultural e política. Segundo este autor, a apropriação desigual da técnica perpetua relações coloniais e a subordinação do continente africano (Diop, 1987, p. 56).

Nesse sentido, a biometria pode ser interpretada como prolongamento da lógica colonial: dados corporais de populações de África e do Sul global são extraídos e armazenados em servidores controlados por centros hegemônicos. A colonialidade do poder tecnológico aparece, portanto, na forma como a biometria transforma identidades em recursos a serem explorados.

A ilusão da solução tecnológica

Muito bem, quão sábio foi Evgeny Morozov (2011) ao denunciar o que denomina de "solucionismo tecnológico": a crença de que problemas políticos e sociais podem ser resolvidos unicamente por dispositivos técnicos. Para o autor, essa visão legitima formas sofisticadas de vigilância e desresponsabiliza os atores políticos (Morozov, 2011, p. 45). A biometria insere-se nesse quadro como um suposto remédio contra fraude e insegurança digital, mas que na prática amplia o poder de monitoramento e controle social. O discurso da segurança, portanto, opera como máscara ideológica para práticas que corroem a própria noção de liberdade e cidadania digital.

A desumanização na modernidade tecnológica

Frantz Fanon (1961) analisou como a colonialidade se sustenta pela objetificação dos corpos, que são reduzidos a instrumentos de poder. Para ele, a violência colonial não é apenas física, mas simbólica e estrutural, convertendo sujeitos em coisas (Fanon, 1961, p. 92). A biometria, nesse sentido, pode ser lida como continuidade dessa lógica: o corpo não é mais apenas marcado pela raça ou pela dominação direta, mas codificado em padrões numéricos que definem quem pode ou não pode participar do espaço digital. Tal codificação implica uma forma de barbárie contemporânea, pois transforma a promessa da internet em mecanismo de segregação.

A centralidade dos direitos humanos na era digital de Henkin e a efetividade dos direitos na era tecnológica em Bobbio

Muito bem, o grande problema e o paradoxo sempre foram como se poderão proteger os direitos humanos, sobretudo, numa sociedade digital como a nossa, — Segundo Bobbio (1992):

> O problema fundamental em relação aos direitos do homem, hoje, não é tanto o de justificá-los, mas o de protegê-los. Trata-se de um problema não filosófico, mas político. Um problema de garantia, não de fundamento. Os direitos naturais são direitos históricos, ou seja, nascem em certas circunstâncias, caracterizadas por lutas em defesa de novas liberdades contra velhos poderes, e nascem de modo gradual, não todos de uma vez e nem de uma vez por todas (Bobbio, 1992, p. 5).

Daí que, a discussão sobre biometria e vigilância não pode ser dissociada do quadro normativo internacional que assegura a dignidade da pessoa humana. Louis Henkin (1990), um dos mais renomados juristas a tratar do tema, argumenta que a Declaração Universal dos Direitos Humanos constitui "a Constituição da comunidade internacional" (Henkin, 1990, p. 18). Para o autor, os direitos consagrados pela ONU — como a liberdade, a privacidade e a igualdade — representam limites inegociáveis ao exercício do poder político e tecnológico. Nesse sentido, o uso indiscriminado da biometria como condição de acesso digital pode configurar violação direta a esses princípios fundamentais, transformando a internet em um espaço de barbárie institucionalizada.

Na mesma linha de pensamento, Norberto Bobbio (1992), em sua obra *A era dos direitos*, enfatiza que o grande desafio contemporâneo não é mais fundamentar teoricamente os direitos humanos, mas sim assegurar a sua efetividade. Para o autor, "o problema fundamental em relação aos direitos do homem, hoje, não é tanto justificá-los, mas protegê-los" (Bobbio, 1992, p. 25). Essa afirmação revela-se particularmente atual diante das novas formas de vigilância digital. A biometria, apresentada como instrumento de segurança e modernização, pode se tornar um obstáculo à efetividade desses direitos quando utilizada para restringir o acesso, hierarquizar usuários ou vigiar permanentemente cidadãos. Nesse sentido, a crítica de Bobbio ajuda a evidenciar que a mera proclamação normativa dos direitos, como nos documentos da ONU, não é suficiente: é necessário um esforço político e institucional para impedir que tecnologias de controle convertam a internet em uma sociedade bárbara.

Convergência marco-teórica

Em boa verdade, a análise crítica da biometria como pretexto de falência global da internet exige um enquadramento teórico plural, capaz de articular dimensões tecnológicas, políticas, coloniais e jurídicas. Castells (1999) mostra que a sociedade em rede é estruturada por fluxos de informação controlados por quem detém poder sobre os códigos e nós digitais.

Nesse contexto, a biometria surge como filtro central de acesso, convertendo corpos em senhas e instituindo exclusões. Diop (1987), por sua vez, alerta que a técnica não é neutra, mas carregada de colonialidade. A imposição de tecnologias biométricas em países do Sul global prolonga a subordinação histórica, pois dados corporais passam a ser extraídos e controlados por centros hegemônicos, em clara continuidade do colonialismo científico. Fanon (1961) aprofunda essa crítica ao demonstrar como a modernidade converte corpos em objetos de dominação; a biometria atualiza essa lógica ao reduzir identidades humanas a padrões numéricos, reiterando processos de desumanização. Por outro lado, Morozov (2011) acrescenta que a legitimação da biometria se dá pelo "solucionismo tecnológico", um discurso que apresenta dispositivos digitais como respostas inquestionáveis a problemas sociais, mascarando os riscos de vigilância permanente. É nesse ponto que a contribuição de Henkin (1990) e Bobbio (1992) torna-se fundamental: ambos sublinham que os direitos humanos, proclamados universalmente pela ONU, só têm sentido se forem protegidos e efetivos. A biometria, ao limitar a liberdade e a igualdade de acesso, pode violar diretamente esses princípios fundamentais, transformando a promessa da internet em barbárie institucionalizada.

Com base nessas afirmações, os seis autores convergem para um diagnóstico comum: a biometria, longe de ser mera ferramenta técnica, configura-se como dispositivo político e ideológico de vigilância, exclusão e hierarquização digital. A articulação entre rede (Castells), colonialidade (Diop e Fanon), ilusão tecnológica (Morozov) e direitos humanos (Henkin e Bobbio) permite compreender que o desafio não é apenas técnico, mas civilizatório. A internet, que deveria ser espaço de emancipação, corre o risco de se converter em arena bárbara, onde os corpos são reduzidos a códigos e a dignidade humana é subordinada ao controle algorítmico.

A Biometria

Bem, podemos começar por definir da seguinte maneira:

"Biometria refere-se à ciência de estabelecer a identidade de um indivíduo com base em características físicas ou comportamentais intrínsecas, como impressões digitais, reconhecimento facial, íris e padrões de voz" (Jain, Ross, & Prabhakar, 2004, p. 1).

Para Maltoni, Maio, Jain e Prabhakar (2009): "A biometria fornece meios automáticos de reconhecimento pessoal com alto grau de confiabilidade, sendo considerada um dos pilares da segurança moderna" (p. 3). E na mesma linha de definição, Ratha, Connell e Bolle (2001): "O reconhecimento biométrico oferece a promessa de uma identificação precisa, mas carrega consigo riscos de usabilidade, privacidade e possíveis formas de abuso" (p. 4). De acordo com Wayman (2000): "A biometria[5] é o uso de medições estatísticas de características fisiológicas ou comportamentais para verificar ou determinar a identidade de indivíduos" (p. 93).

A internet

Pode-se dizer que, "A internet é, ao mesmo tempo, a espinha dorsal da comunicação global e o espaço por onde circulam as redes de informação que estruturam a nova economia, a política e a cultura" (Castells, 2001, p. 1). No que significa que a internet não é só tecnologia; é a base que conecta o mundo todo, mudando como funcionam a economia, a política e a cultura. Por isso, de acordo com Lévy (1999),"A internet constitui um espaço virtual de comunicação interativa e coletiva, em que se formam novas modalidades de conhecimento e sociabilidade" (p. 107). Dito de outro modo, a internet é um espaço onde as pessoas interagem e criam conhecimento juntas, transformando as formas de viver em sociedade.

O conceito de vigilância

Muito bem, a vigilância é o ato de observar e controlar pessoas ou grupos para garantir ordem, segurança ou poder. Hoje, isso vai muito além do policial na rua. A internet, as câmeras e a biometria transformaram a vigilância num processo automático e invisível.

[5] Estamos a tentar dizer que, Jain, Ross e Prabhakar (2004), Maltoni et al. (2009), Ratha, Connell e Bolle (2001) e Wayman (2000) entendem convergencialmente de que a biometria é uma forma de identificar pessoas usando características únicas do corpo ou do comportamento — como digital, rosto, íris ou voz. De que a biometria é vista como uma ferramenta moderna para dar mais segurança, porque torna difícil falsificar ou imitar a identidade de alguém. De que apesar de ser precisa, a biometria traz riscos: pode violar a privacidade das pessoas e ser usada de forma abusiva. De que a biometria mede estatisticamente partes do corpo ou comportamentos para confirmar ou descobrir quem é uma pessoa.

Para Lyon (2007): "A vigilância pode ser definida como o processo de monitoramento rotineiro de populações inteiras ou de grupos sociais específicos, utilizando dados pessoais para fins de gestão, proteção ou controle" (p. 14). Segundo Foucault, "vigiar é um mecanismo fundamental do poder disciplinar, que se exerce por meio da observação contínua, invisível e hierárquica, organizando os corpos e as condutas" (Foucault, 1975, p. 172).

Vale a pena dizer que, no mundo digital, a vigilância virou permanente e difusa. Basta um clique, um login com reconhecimento facial ou o uso de impressões digitais para que rastros sejam guardados e analisados. O discurso da segurança é o argumento mais usado para justificar, mas o efeito é que os cidadãos ficam cada vez mais expostos e vulneráveis.

O que é barbárie?

A barbárie é a perda ou destruição da dignidade humana. Acontece quando a técnica, o poder ou a violência se sobrepõem ao respeito pelos direitos humanos e pela vida.

Conforme Adorno e Horkheimer (1947/1985), "a barbárie não consiste em retornar a um estado primitivo, mas em repetir, sob formas cada vez mais técnicas e avançadas, a desumanização do homem" (p. 32). Para Diop (1987): "Barbárie é a negação do projeto civilizatório africano e humano, substituído por práticas de dominação que desfiguram a dignidade do homem e apagam sua memória histórica" (Diop, 1987, p. 45).

A Exclusão digital

Com efeito, segundo Warschauer (2003): "Exclusão digital não é apenas a falta de acesso físico às tecnologias de informação e comunicação, mas também a ausência de habilidades, conteúdos relevantes e apoio social necessários para utilizá-las de forma significativa" (p. 6). De acordo com Norris, "a exclusão digital expressa a divisão entre aqueles que têm acesso e capacidade de usar as novas tecnologias da informação e aqueles que permanecem desconectados, ampliando desigualdades sociais já existentes" (Norris, 2001, p. 4).

Nestes moldes, a exclusão digital é quando uma parte da população fica de fora do acesso e do uso real das tecnologias de informação e comunicação. Não é só não ter internet ou computador. É também não ter as condições para usar: falta de formação, conteúdos pouco relevantes, barreiras linguísticas, custos altos e até falta de energia elétrica em certas regiões. Na prática, quem sofre exclusão digital não consegue participar plenamente da vida social, econômica, política e cultural que hoje depende fortemente da internet. Isso amplia desigualdades já existentes — quem está dentro da rede tem mais oportunidades; quem está fora fica ainda mais marginalizado.

METODOLOGIA UTILIZADA

Com efeito, a presente investigação insere-se no campo das ciências sociais aplicadas, adotando uma abordagem qualitativa, exploratória e crítica. Segundo Flick (2009), a pesquisa qualitativa busca compreender fenómenos complexos em seus contextos, privilegiando a interpretação de significados (Flick, 2009, p. 21). Essa abordagem é particularmente adequada para analisar o impacto da biometria na internet, visto que o problema não é apenas técnico, mas envolve dimensões políticas, éticas e civilizatórias.

O método empregado é o da análise documental e bibliográfica crítica. De acordo com Gil (2008), a pesquisa bibliográfica consiste em examinar contribuições anteriores sobre o tema, permitindo identificar lacunas e formular novos problemas de investigação (Gil, 2008, p. 50). Assim, o corpus teórico integra autores clássicos e contemporâneos que tratam da sociedade em rede, da colonialidade, do solucionismo tecnológico e dos direitos humanos: Castells (1999), Diop (1987), Morozov (2011), Fanon (1961), Henkin (1990) e Bobbio (1992).

Por conseguinte, a análise segue uma perspectiva crítica e interdisciplinar. Conforme Minayo (2012), o enfoque crítico possibilita problematizar os fenómenos sociais para além de sua aparência imediata, evidenciando as contradições que os sustentam (Minayo, 2012, p. 45). Nesse sentido, a biometria é investigada não apenas como recurso técnico de segurança, mas como dispositivo de exclusão e vigilância, correlacionando-a com a possibilidade de violação de direitos humanos fundamentais, consagrados pela Declaração Universal dos Direitos Humanos (ONU, 1948/1998, p. 72).

Portanto, a metodologia adotada é teórica, analítica e crítica, orientada por fontes bibliográficas e documentais. O objetivo é evidenciar como a biometria, sob o pretexto de segurança, reforça a barbárie digital e compromete a efetividade dos direitos humanos.

DISCUSSÃO DOS RESULTADOS

A biometria e o discurso da segurança e exclusão digital

Decerto, o discurso dominante associa a biometria à segurança e à proteção contra crimes digitais. Entretanto, como apontam Foucault (1975) e Zuboff (2019), a lógica securitária frequentemente serve de legitimação para práticas de vigilância massiva. O que se apresenta como "segurança" converte-se em monitorização permanente, restringindo a autonomia individual.

Por isso é que a exigência de credenciais biométricas não é universalmente acessível. Por exemplo, populações marginalizadas, sem documentação formal ou com acesso precário a tecnologias, são excluídas da cidadania digital. A internet, em vez de inclusiva, converte-se em espaço de exclusão. A biometria naturaliza a desigualdade, criando um fosso entre os "aptos" e os "inaptos" à identificação. A biometria, apresentada como solução universal de autenticação, esconde assimetria tecnológica profunda. Sua implementação, de facto, pressupõe infraestrutura de alta complexidade: câmeras de alta resolução, scanners ópticos, sensores de impressão digital, algoritmos de aprendizado profundo e bases de dados massivas. Esses requisitos colocam em desvantagem populações e países que não dispõem de recursos financeiros, técnicos e humanos para implantar ou acessar tais sistemas.

Do ponto de vista informático, a exclusão se materializa em três níveis principais:

1. *Infraestrutural* – A coleta e o processamento de dados biométricos exigem conectividade robusta (rede 4G/5G ou fibra óptica), *data centers* com elevada capacidade de armazenamento e servidores de alto desempenho. Em regiões periféricas, onde a conectividade ainda é instável e os custos de acesso são altos, a própria exigência de biometria para acesso a serviços digitais cria barreiras adicionais (Castells, 2003).

2. *Algorítmica* – Os algoritmos de reconhecimento facial e de voz são treinados com bases de dados predominantemente eurocêntricas. Isso gera vieses técnicos que resultam em taxas mais elevadas de erro para populações negras, indígenas, mulheres e idosos (Buolamwini & Gebru, 2018). O problema não é apenas de exclusão de acesso, mas de inclusão desigual: mesmo quando os indivíduos conseguem acessar o sistema, sua experiência é marcada pela falha e pelo erro sistemático.
3. *Jurídico-político* – A interoperabilidade de bancos de dados biométricos, muitas vezes administrados por empresas transnacionais, cria dependência tecnológica em países africanos e do Sul global. Essa condição enfraquece a soberania digital, uma vez que informações sensíveis de milhões de cidadãos passam a ser processadas e armazenadas fora do território nacional (Carvalho, 2004; Kajibanga, 2000).

Por isso é que a exclusão digital não é um efeito colateral, mas um produto estrutural da biometria. De boa memória, Fanon (2005) já havia apontado que sistemas classificatórios não são neutros: eles são construídos para separar os "aptos" dos "não aptos". A lógica biométrica perpetua essa divisão, ao transformar a ausência de documentação ou a falha do algoritmo em sinónimo de inexistência digital. Na mesma linha de abordagem, Quijano (2000) contribui para a compreensão desse fenómeno ao propor a noção de colonialidade do poder: tecnologias aparentemente modernas reatualizam hierarquias históricas. Na prática, a biometria reforça um dualismo global — de um lado, cidadãos plenos, identificáveis e integrados; de outro, sujeitos precários, invisíveis e descartáveis.

Daí que, em termos tecnológicos, essa desigualdade é agravada pelo modelo de negócios das grandes plataformas digitais. Muitos serviços biométricos estão associados a sistemas de autenticação oferecidos por empresas como *Microsoft, Amazon ou Huawei*, que operam sob lógica de mercado e não de inclusão social. Ou seja, o acesso biométrico não depende apenas de infraestrutura, mas de capacidade de pagamento e adesão ao ecossistema corporativo global.

Nesses moldes, a biometria não apenas amplia a exclusão digital já existente, mas institui uma forma de "apartheid informático[6]", em que a participação na vida digital depende da posse de credenciais biométricas reconhecidas por sistemas globais.

A internet em colapso: da rede ao muro

Infelizmente, a universalidade da internet está em erosão. Já se pode dizer que o projeto universalista da internet cede espaço a muros digitais erigidos pela biometria. O acesso deixa de ser direito universal e passa a depender de autenticação permanente.

Han (2017) chama esse processo de "sociedade da transparência", em que a exposição integral da identidade se torna pré-condição para participação. Nesse cenário, a internet não desaparece tecnicamente, mas morre simbolicamente como promessa de liberdade e emancipação. Este processo de colapso da internet faz-nos propor a ideia central de falência global da internet, entendido como colapso de seus fundamentos democráticos. A rede deixa de ser espaço aberto para tornar-se aparato de controle identitário. O ideal fundador da internet era o de uma rede aberta, descentralizada e sem fronteiras, baseada no princípio da interoperabilidade. Tecnicamente, o protocolo TCP/IP foi concebido para garantir comunicação universal entre dispositivos heterogêneos, independentemente de localização ou jurisdição (Leiner et al., 2009). Esse caráter universalista sustentou a narrativa da internet como "rede das redes", espaço de circulação livre da informação e do conhecimento.

Não obstante, a implementação da biometria como requisito de acesso está produzindo uma transformação radical dessa arquitetura. A autenticação biométrica introduz barreiras identitárias que segmentam a rede em espaços fechados, condicionando a entrada e a permanência à verificação permanente da identidade. Esse processo equivale, em termos técnicos, a uma firewallização social da internet: se antes os muros eram erguidos para proteger infraestruturas críticas, agora eles são projetados para separar sujeitos "legítimos" de sujeitos "ilegítimos". A falência global da internet como projeto universal decorre da articulação de três camadas tecnológicas:

[6] Termo usado nesse artigo para designar, a grosso modo, uma terrível e absurda exclusão e segregação digital.

1. *Arquiteturas de autenticação centralizada* – Sistemas como *Single Sign-On* (SSO) baseados em biometria, oferecidos por grandes corporações (Google Identity, Microsoft Entra ID, Amazon Cognito), funcionam como portais de acesso que controlam múltiplos serviços. Essa centralização concentra poder e cria "zonas muradas" da rede.
2. *Redes de vigilância em tempo real* – A expansão do 5G e da *Internet das Coisas* (IoT) permite que câmeras e sensores transmitam dados biométricos em fluxo contínuo para nuvens corporativas. Isso viabiliza a criação de sistemas de controle pervasivo, nos quais a mobilidade digital e física do indivíduo é constantemente monitorada (Brayne, 2021).
3. *Geopolítica da soberania digital* – Países e blocos regionais vêm impondo legislações de identificação digital obrigatória, como o *Digital ID* da União Europeia, o *Aadhaar* na Índia e iniciativas emergentes em África. Essas políticas, quando acopladas à biometria, criam muros geopolíticos na rede, pois o acesso global passa a depender do cumprimento de normas nacionais específicas (Kuner, 2021).

E, infelizmente, a consequência dessa dinâmica é que a internet deixa de ser um espaço universal e passa a operar como um ecossistema murado (*walled garden*). Os serviços digitais tornam-se compartimentalizados, exigindo autenticações distintas e biométricas para cada ambiente, reduzindo a interoperabilidade e aumentando a dependência de plataformas proprietárias. Esse movimento é comparável ao que Byung-Chul Han (2017) chama de "sociedade da transparência", em que a participação está condicionada à exposição integral da identidade, conforme já dito acima. Porém, na lógica informático-tecnológica, trata-se de uma involução arquitetural: de uma rede projetada para interconexão universal para uma rede segmentada por credenciais de acesso.

Daí que, a falência não é acidente, mas resultado de escolhas tecnológicas e políticas que convertem o princípio da interoperabilidade em princípio de exclusão identitária.

Diante disso, é imperioso dizer que a pesquisa perguntou inicialmente: *a biometria funciona como pretexto para a falência global da internet, instaurando uma nova forma de sociedade bárbara?*

As análises realizadas permitem afirmar que as hipóteses formuladas foram confirmadas em função da perguntada levantada.

1. *Hipótese 1 – A biometria legitima a vigilância sob o discurso da segurança.* Confirmou-se que o uso da biometria não se limita à autenticação de identidades, mas funciona como instrumento de monitoramento permanente, reforçando práticas de controle social. Lyon (2007) sustenta que a vigilância de populações inteiras tornou-se uma rotina política e económica (p. 14), enquanto Foucault (1975) demonstra que vigiar é um mecanismo estrutural do poder disciplinar (p. 172). Assim, a biometria atua como extensão desses dispositivos.

2. *Hipótese 2 – A biometria aprofunda a exclusão digital e reforça desigualdades estruturais.*

   Os resultados apontam que, em contextos de desigualdade socioeconómica, a exigência de acesso biométrico agrava a marginalização de grupos sem recursos tecnológicos adequados. Norris (2001) descreve que o fosso digital amplia desigualdades sociais (p. 4), e Warschauer (2003) mostra que exclusão não é só falta de acesso, mas também ausência de competências e conteúdos significativos (p. 6). Isso confirma a hipótese de que a biometria pode transformar-se em barreira de exclusão.

3. *Hipótese 3 – A biometria ameaça os direitos humanos fundamentais.* A pesquisa mostrou que a coleta massiva e compulsória de dados biométricos coloca em risco a proteção da dignidade e da privacidade, direitos consagrados na Carta das Nações Unidas (ONU, 1948/1998, p. 72). Nesse sentido, Henkin (1990) já advertia que o desafio contemporâneo não é justificar os direitos, mas garantir sua efetividade (p. 4). Bobbio (1992) complementa que o problema central não é filosófico, mas político, pois os direitos devem ser protegidos contra a erosão (p. 5).

Deste modo, confirma-se que a pergunta de pesquisa encontra resposta positiva: a biometria, sob a justificativa de segurança, funciona como pretexto ideológico que fragiliza o projeto emancipatório da internet, promove novas formas de exclusão e pavimenta a emergência de uma sociedade bárbara digital, como denunciado por Adorno e Horkheimer (1985, p. 32) e Diop (1987, p. 45).

A sociedade bárbara

Ora pois, denominamos "sociedade bárbara" o resultado desse processo: um regime em que a tecnologia, em vez de emancipar, subjuga; em que a internet, em vez de abrir horizontes, fecha fronteiras. Essa barbárie não é retorno ao primitivo, mas barbárie tecnocrática – altamente sofisticada, porém incapaz de garantir a dignidade humana. A noção de "sociedade bárbara" descreve o regime emergente: tecnocrático, sofisticado e excludente. A barbárie aqui não significa ausência de técnica, mas sim regressão política travestida de modernidade.

Repare que, Kilomba (2008) demonstra como o racismo se atualiza sob novas roupagens, permanecendo estrutural nas relações de poder. A sociedade bárbara traduz essa atualização: exclusão e violência justificadas pela biometria. Diop (1974/1991) enfatiza que a verdadeira modernidade africana deve ser emancipatória e autônoma. A biometria, ao contrário, configura-se como modernidade parasitária, que extrai dados e identidades sem garantir dignidade ou liberdade.

O conceito de sociedade bárbara, neste contexto, não remete à ausência de tecnologia, mas à sua utilização como instrumento de exclusão, desumanização e regressão civilizatória. Paradoxalmente, quanto mais sofisticados se tornam os sistemas informáticos, mais eles podem ser apropriados para práticas de controle e marginalização. A barbárie não é o contrário da técnica: é o seu uso distorcido.

Os sistemas de inteligência artificial aplicados ao reconhecimento biométrico (*deep learning, redes neurais convolucionais, modelos de linguagem multimodal*) funcionam com base em grandes bases de dados (datasets). Quando esses dados carregam vieses raciais, de gênero e de classe, a tecnologia reproduz e amplia as desigualdades. Buolamwini e Gebru (2018) demonstraram que algoritmos de reconhecimento facial apresentam erros sistematicamente maiores para rostos de pessoas negras e mulheres. Essa falha técnica gera uma forma de barbárie informacional: sujeitos inteiros passam a ser estatisticamente descartáveis. A classificação algorítmica decide quem pode acessar um serviço, transitar numa fronteira ou até provar sua existência jurídica.

Efetivamente, em uma sociedade bárbara digital, os dados não são tratados como bem comum, mas como armas estratégicas. A coleta massiva de informações biométricas, associada a tecnologias de *big data* e *cloud computing*, cria arsenais de controle que podem ser usados contra populações inteiras. Zuboff (2019) chama isso de "capitalismo de vigilância", em que cada gesto do usuário é extraído, armazenado e processado como mercadoria.

A barbárie se manifesta quando esses sistemas não visam à proteção do cidadão, mas à antecipação e controle de comportamentos considerados "indesejados". É o uso bélico da informação em tempos de paz. O discurso tecnocrático legitima a exclusão sob a aparência de neutralidade científica. A biometria, apoiada em fórmulas matemáticas e protocolos informáticos, cria a ilusão de objetividade. No entanto, como alerta Diop (1981), toda técnica é produto de um contexto histórico e social, carregando consigo relações de poder.

A barbárie digital não é fruto da ausência de racionalidade, mas do seu excesso instrumental: a racionalidade técnica que se sobrepõe à dignidade humana. Em vez de emancipar, os sistemas informáticos tornam-se mecanismos de seleção e segregação. Na sociedade bárbara, o ser humano deixa de ser sujeito para ser reduzido a um vetor de dados. Impressões digitais, padrões faciais, cadência de voz e histórico de navegação compõem perfis codificados que substituem identidades reais. A existência jurídica e social passa a depender do reconhecimento algorítmico. Em termos informáticos, isso significa que a cidadania é condicionada ao código: se o sistema aceita, o indivíduo existe; se o sistema falha, o indivíduo desaparece. Essa dependência cria uma forma inédita de barbárie, em que a exclusão não é decretada por exércitos ou burocratas, mas por falhas silenciosas de software.

A sociedade bárbara é aquela em que a tecnologia, em vez de universalizar direitos, institui um novo tipo de apartheid digital, baseado na biometria, na vigilância algorítmica e na tecnocracia corporativa. O resultado é um retrocesso civilizatório: a substituição da convivência social pelo controle absoluto mediado por máquinas.

CONSIDERAÇÕES FINAIS

Em guisa de conclusão, podemos afirmar que a biometria, apresentada como inovação, revela-se dispositivo central de exclusão, vigilância e controle. O risco iminente é a falência global da internet enquanto espaço livre, conduzindo ao que denominamos sociedade bárbara. O enfrentamento dessa tendência exige alternativas tecnológicas baseadas em direitos, transparência e inclusão. Por isso, o artigo demonstrou que a biometria, embora apresentada como tecnologia de segurança e confiabilidade, constitui-se em dispositivo de vigilância e exclusão. A análise confirmou as hipóteses levantadas: primeiro, ao mostrar que a biometria legitima práticas de monitoramento contínuo, inscritas no quadro de poder disciplinar descrito por Foucault (1975) e no conceito de vigilância de massas apontado por Lyon (2007); segundo, ao evidenciar que o acesso biométrico aprofunda desigualdades sociais e tecnológicas, como advertido por Norris (2001) e Warschauer (2003); e, terceiro, ao demonstrar que a coleta e uso indiscriminado de dados biométricos fragilizam a proteção de direitos humanos fundamentais, tema central nas reflexões de Henkin (1990) e Bobbio (1992).

Além disso, o estudo destacou que a internet, outrora pensada como espaço democrático de circulação do conhecimento (Castells, 2001; Lévy, 1999), sofre crescente captura por forças estatais e corporativas. Essa dinâmica conduz à emergência de uma sociedade bárbara digital, onde a técnica substitui o humano, a vigilância suplanta a liberdade e a exclusão torna-se regra. Adorno e Horkheimer (1985) já advertiam que a barbárie não é retorno ao primitivo, mas a repetição da desumanização sob novas formas; Diop (1987) complementa que essa barbárie é a negação do projeto civilizatório humano.

Assim sendo, conclui-se que a biometria opera como pretexto ideológico e político para a erosão do projeto emancipatório da internet. A promessa de inclusão e democratização dá lugar a práticas que comprometem a privacidade, a dignidade e os direitos humanos.

Diante desse quadro, este artigo propõe que a crítica acadêmica à biometria deve permanecer vigilante, pois apenas pela denúncia sistemática e pela defesa ativa dos direitos fundamentais será possível evitar que o espaço digital global se consolide como território de exclusão e de barbárie tecnológica.

REFERÊNCIAS BIBLIOGRÁFICAS

Adorno, T. W., & Horkheimer, M. (1985). *Dialética do esclarecimento: Fragmentos filosóficos* (G. A. Almeida, Trad.). Jorge Zahar. (Trabalho original publicado em 1947)

Bobbio, N. (1992). *A era dos direitos*. Campus.

Castells, M. (1999). *A sociedade em rede* (Vol. 1). Paz e Terra.

Castells, M. (2001). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press.

Diop, C. A. (1987). *Civilization or barbarism: An authentic anthropology*. Lawrence Hill Books.

Fanon, F. (1961). *Les damnés de la terre*. Éditions Maspero.

Flick, U. (2009). *Introdução à pesquisa qualitativa* (3.ª ed.). Artmed.

Foucault, M. (1975). *Surveiller et punir: Naissance de la prison*. Gallimard.

Gil, A. C. (2008). *Métodos e técnicas de pesquisa social* (6.ª ed.). Atlas.

Henkin, L. (1990). *The age of rights*. Columbia University Press.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20. https://doi.org/10.1109/TCSVT.2003.818349

Lévy, P. (1999). *Cibercultura*. Editora 34.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition* (2nd ed.). Springer.

Minayo, M. C. S. (2012). *O desafio do conhecimento: Pesquisa qualitativa em saúde* (13.ª ed.). Hucitec.

Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. PublicAffairs.

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge University Press.

Organização das Nações Unidas. (1998). *Declaração Universal dos Direitos Humanos* (Texto original de 1948). Cadernos do Povo.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634. https://doi.org/10.1147/sj.403.0614

Warschauer, M. (2003). *Technology and social inclusion: Rethinking the digital divide*. MIT Press.

Wayman, J. L. (2000). Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics, 1*(1), 93–113. https://doi.org/10.1142/S0219467801000051