RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano IV, v.1, n.1, ago/dez 2024.| submissão: 23/08/2024 | aceito: 25/08/2024 | publicação:27/08/2024

Cibersegurança Algorítmica e a Era da Autodefesa Digital: Caminhos para uma Nova Cidadania Cibernética

Algorithmic Cybersecurity and the Age of Digital Self-Defense: Pathways to a New Cyber Citizenship

Lucas Pereira de Souza

Graduado em Ciência da Computação, Universidade dos Guararapes.

RESUMO

Este artigo propõe uma reflexão profunda sobre a cibersegurança contemporânea, focando no papel da inteligência algorítmica e sua influência na soberania digital dos indivíduos. Ao abordar desde a arquitetura de vigilância baseada em dados até os desafios éticos da automação da defesa cibernética, este estudo convida à construção de uma nova cidadania digital crítica e consciente. Utiliza-se como metodologia a pesquisa bibliográfica e documental, com enfoque interdisciplinar, envolvendo os campos da tecnologia, sociologia, direito e filosofia da informação. O texto propõe o conceito de "autodefesa digital algorítmica" como chave para enfrentar os riscos emergentes da era da hiperconectividade, protegendo não apenas sistemas, mas sobretudo a dignidade e a liberdade dos usuários.

Palavras-chave: Cibersegurança; Algoritmos; Cidadania Digital; Autodefesa; Privacidade; Vigilância.

ABSTRACT

This article proposes an in-depth reflection on contemporary cybersecurity, focusing on the role of algorithmic intelligence and its influence on individuals' digital sovereignty. By addressing themes ranging from data-driven surveillance architectures to the ethical challenges of automated cyber defense, this study invites the construction of a new, critical, and conscious digital citizenship. The methodology is based on bibliographic and documentary research, with an interdisciplinary approach encompassing the fields of technology, sociology, law, and information philosophy. The text introduces the concept of "algorithmic digital self-defense" as a key strategy for confronting the emerging risks of the hyperconnected era, aiming to protect not only systems, but above all, the dignity and freedom of users.

Keywords: Cybersecurity; Algorithms; Digital Citizenship; Self-Defense; Privacy; Surveillance.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

1 - Introdução à Cibersegurança Algorítmica

A cibersegurança, tradicionalmente compreendida como o conjunto de práticas para proteger sistemas e dados, evoluiu significativamente nas últimas décadas. A complexidade das ameaças contemporâneas exige uma nova lente interpretativa, que não se restrinja ao campo técnico, mas considere aspectos sociopolíticos e éticos da proteção digital. Nesse contexto, os algoritmos emergem como atores centrais da segurança digital, automatizando decisões de defesa e, por vezes, também de ataque, com base em padrões de comportamento detectados em tempo real.

A expansão dos dispositivos conectados, a internet das coisas (IoT) e os sistemas autônomos transformaram radicalmente o cenário de vulnerabilidades cibernéticas. Hoje, ataques não ocorrem apenas por ação humana direta, mas muitas vezes por falhas ou manipulações em sistemas de inteligência artificial (IA). A segurança deixou de ser um domínio restrito a administradores de rede e tornou-se uma pauta pública, que toca diretamente a vida cotidiana de cidadãos conectados.

Nesse cenário, surge a noção de "cidadania cibernética" — um conceito que transcende o direito ao acesso digital e inclui a capacidade de compreender, decidir e agir frente a riscos algorítmicos. A segurança digital passa, então, a ser não apenas uma questão técnica, mas um direito civil essencial, em meio ao ambiente de vigilância massiva e manipulação algorítmica.

Ao mesmo tempo, o volume e a velocidade de dados tratados por sistemas inteligentes tornam obsoletos os modelos tradicionais de resposta. Firewalls e antivírus isolados já não bastam. Novas abordagens, como a detecção comportamental preditiva e os sistemas de resposta autônoma, representam avanços, mas também suscitam preocupações éticas: quem é responsável quando um algoritmo bloqueia um usuário inocente ou permite uma brecha crítica?

Este artigo defende que, diante dessa nova realidade, é preciso promover a autodefesa digital algorítmica, entendida como a capacidade de usuários, organizações e Estados de compreenderem e intervirem de forma crítica e ética nos sistemas que gerenciam sua própria segurança. Essa proposta visa empoderar indivíduos não apenas como consumidores de tecnologia, mas como agentes ativos de proteção de seus próprios dados, identidades e decisões.

A construção dessa nova abordagem exige não apenas inovação tecnológica, mas também uma educação crítica em segurança digital e uma política de regulação transparente e inclusiva. A seguir, serão exploradas as bases técnicas, os desafios éticos e as perspectivas para o fortalecimento da cibersegurança algorítmica como caminho para uma nova cidadania digital.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

2. Vigilância Automatizada e os Paradoxos da Liberdade Digital

A ascensão da vigilância digital automatizada configura um dos fenômenos mais impactantes da era informacional. Diferente da vigilância clássica, centrada em observadores humanos e limitada pela capacidade física de acompanhamento, o monitoramento algorítmico opera em escala global, ininterrupta e silenciosa. Plataformas digitais, sistemas operacionais, assistentes virtuais e até eletrodomésticos inteligentes se tornaram pontos de coleta contínua de dados, muitas vezes sem o pleno conhecimento ou consentimento dos usuários. Esse processo cria o que Shoshana Zuboff (2019, EUA) denominou de "capitalismo de vigilância", onde a informação pessoal se transforma em recurso econômico e geopolítico.

Paradoxalmente, esse modelo de monitoramento em tempo real é apresentado como garantia de liberdade e personalização. Usuários, ao receberem conteúdos, anúncios e serviços "sob medida", são levados a crer que estão no controle de suas experiências digitais. No entanto, o controle está, na realidade, nas mãos dos algoritmos que processam seus dados, definindo o que será exibido, quais acessos serão permitidos ou bloqueados e até que tipos de interações são possíveis. Trata-se de uma liberdade condicionada, moldada por interesses comerciais e padrões de classificação invisíveis.

O grande risco da vigilância algorítmica não reside apenas na coleta de dados, mas principalmente na forma como esses dados são processados e utilizados. A criação de perfis comportamentais baseados em padrões históricos pode levar à discriminação algorítmica, à exclusão digital ou ao direcionamento ideológico. Em ambientes corporativos, por exemplo, decisões de contratação ou demissão podem ser automatizadas com base em análises de comportamento digital. Em contextos políticos, algoritmos podem ser utilizados para manipular percepções sociais, como ocorreu no escândalo da Cambridge Analytica, revelado em 2018 no Reino Unido e nos Estados Unidos.

A arquitetura dessa vigilância é muitas vezes opaca. Os algoritmos são protegidos como segredos comerciais ou classificados como "incompreensíveis" até mesmo por seus próprios criadores, como no caso dos sistemas de aprendizado profundo. Essa ausência de transparência gera um déficit democrático, no qual cidadãos são monitorados sem saber por quem, por quê e com que finalidade. O princípio do consentimento informado, base do direito à privacidade, torna-se uma formalidade esvaziada, incapaz de conter a voracidade dos sistemas de coleta e análise de dados.

A resposta a esse desafio exige mais do que medidas técnicas de segurança; requer um novo contrato social digital, no qual a cidadania cibernética se constitua como um direito à compreensão e intervenção sobre os sistemas que nos monitoram. Isso inclui o direito à explicação algorítmica, à exclusão de dados, à portabilidade de perfis digitais e ao anonimato em certos contextos. Também demanda ações estatais e multilaterais para garantir que empresas e governos respeitem princípios de proporcionalidade, transparência e responsabilidade.

Portanto, a vigilância algorítmica inaugura uma era de contradições profundas: liberdade digital versus controle automatizado; personalização versus manipulação; segurança versus

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

violação da privacidade. Navegar nesse cenário exige o fortalecimento de uma cultura crítica da informação, onde o cidadão não apenas usa tecnologia, mas compreende e questiona sua arquitetura subjacente. Nas próximas seções, exploraremos como a autodefesa digital pode emergir como uma alternativa estratégica e cidadã frente a esse cenário complexo e desigual.

3. Autodefesa Digital: da Segurança Passiva ao Empoderamento Algorítmico

A noção de autodefesa digital surge como uma reação necessária à passividade imposta pela vigilância algorítmica. Tradicionalmente, os usuários da internet são colocados em posição de vulnerabilidade, dependendo de ferramentas pré-configuradas por corporações ou administradores de sistemas. Nesse modelo, a segurança é algo delegado: o indivíduo confia em terceiros para proteger seus dados, sua navegação e sua identidade online. A proposta da autodefesa digital rompe com essa lógica, defendendo que o usuário deve ser sujeito ativo no processo de proteção cibernética, dotado de conhecimento, recursos e poder de decisão sobre o ambiente digital que habita.

A autodefesa digital algorítmica se diferencia das práticas convencionais de cibersegurança ao não se limitar à instalação de softwares ou ao uso de senhas robustas. Ela implica uma mudança de postura: exige consciência crítica sobre como os algoritmos funcionam, quais dados são coletados, para que fins são utilizados e quais são os impactos dessas decisões sobre a autonomia e os direitos individuais. É, portanto, uma prática informada e política, que aproxima o campo técnico da cidadania digital. Como aponta Morozov (2013, EUA), a verdadeira segurança não está em evitar riscos a qualquer custo, mas em saber navegar e confrontar os sistemas de poder digital com inteligência e estratégia.

Esse tipo de defesa demanda, necessariamente, educação em cibersegurança desde os níveis escolares. É urgente incluir no currículo educacional temas como privacidade digital, rastros informacionais, funcionamento básico de algoritmos, criptografia pessoal e direitos digitais. A literacia digital precisa ir além do uso instrumental das ferramentas e capacitar os indivíduos a reconhecerem ameaças, reagirem a abusos e criarem rotinas próprias de proteção. Essa educação deve também abordar os aspectos éticos da tecnologia, ajudando a formar usuários que não apenas se protejam, mas também respeitem a integridade de outros no ambiente digital.

A tecnologia, por sua vez, deve ser desenhada para fomentar essa autonomia. Interfaces intuitivas, relatórios de uso acessíveis, alertas de exposição de dados e painéis de controle transparentes são elementos fundamentais para a construção de um ecossistema de autodefesa digital. A arquitetura de plataformas deveria favorecer o empoderamento do usuário, e não sua submissão algorítmica. Iniciativas como a criptografia ponta-a-ponta em aplicativos de mensagens ou os navegadores focados em privacidade, como o Tor e o Brave, são exemplos de ferramentas que alinham tecnologia e autonomia cidadã.

Contudo, o acesso a esse tipo de recurso ainda é desigual. Populações vulneráveis, especialmente em regiões periféricas ou países com baixa alfabetização digital, estão mais expostas a ataques e manipulações. Para que a autodefesa digital seja uma prática universal e eficaz, ela precisa ser também inclusiva. Isso implica políticas públicas de acesso a dispositivos seguros, capacitação digital comunitária, incentivo à produção de software livre e campanhas

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

de conscientização que alcancem diferentes grupos sociais. A cibersegurança não pode ser um privilégio de elites tecnológicas; deve ser um direito garantido pelo Estado.

Em suma, a autodefesa digital algorítmica representa um novo paradigma: desloca o foco da dependência institucional para o protagonismo cidadão. Trata-se de um caminho que articula conhecimento, prática e valores democráticos para enfrentar os desafios de um mundo cada vez mais controlado por códigos. A seção seguinte discutirá os limites éticos e jurídicos dessa prática, abordando os dilemas que surgem quando os próprios algoritmos passam a tomar decisões críticas sobre segurança e justiça.

4. Ética, Justiça e a Inteligência Artificial na Cibersegurança

A presença da inteligência artificial (IA) nos sistemas de cibersegurança tem promovido avanços extraordinários, mas também gerado desafios éticos que merecem atenção crítica. Ferramentas baseadas em aprendizado de máquina são hoje capazes de identificar padrões anômalos de tráfego em redes, prever comportamentos suspeitos e bloquear automaticamente acessos potencialmente perigosos. No entanto, ao transferir decisões de segurança para sistemas autônomos, surgem questões fundamentais: quem é o responsável quando um erro ocorre? Qual o limite entre proteção e abuso quando máquinas decidem por nós? A delegação de poder decisório à IA exige, portanto, não apenas confiança técnica, mas fundamentação ética e jurídica clara.

Um dos maiores dilemas reside na opacidade dos algoritmos de segurança. Muitos sistemas de IA operam como "caixas-pretas", ou seja, seus processos decisórios não são transparentes nem auditáveis por seres humanos. Quando uma IA bloqueia um acesso legítimo ou classifica um usuário como ameaça com base em correlações estatísticas, o direito à explicação — princípio defendido pelo Regulamento Geral de Proteção de Dados da União Europeia (2016) — é frequentemente violado. A ausência de clareza sobre como tais decisões são tomadas compromete não apenas a justiça algorítmica, mas também o princípio do devido processo legal em ambientes digitais.

A imparcialidade algorítmica, outro aspecto essencial, também se mostra frágil em sistemas de IA voltados à segurança. Esses algoritmos são treinados com dados históricos, que por sua natureza refletem desigualdades sociais existentes. Isso significa que sistemas de vigilância automatizada podem reforçar vieses discriminatórios, identificando como ameaças padrões de comportamento que se repetem em determinados grupos sociais, especialmente minorias étnicas e populações periféricas. Esse fenômeno já foi identificado em estudos como o de Eubanks (2018, EUA), que mostrou como algoritmos podem ampliar injustiças sociais ao serem utilizados na segurança pública e cibersegurança.

Outro ponto crítico é a autonomia das máquinas. À medida que sistemas de ciberdefesa se tornam mais autônomos, cresce a possibilidade de reações automáticas desproporcionais. Por exemplo, um sistema pode interpretar uma tentativa de acesso indevido como um ataque hostil e acionar contra-ataques automatizados, criando escaladas de conflito digital entre servidores ou até entre países. Em um cenário de guerra cibernética, a decisão de retaliar digitalmente não pode estar inteiramente nas mãos de algoritmos, sob risco de desencadear consequências

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

geopolíticas irreversíveis. A ética da decisão automatizada, portanto, deve ser moldada por protocolos humanos, auditáveis e sujeitos ao controle democrático.

Frente a esses riscos, pesquisadores e juristas têm proposto modelos híbridos de decisão, nos quais a IA atua como sistema de apoio à decisão, e não como juiz autônomo. Nesses modelos, a ação da máquina é revisada por especialistas humanos, que têm o dever de validar ou corrigir suas interpretações. A proposta reforça a ideia de responsabilidade compartilhada e contribui para manter o humano no centro das decisões críticas. No campo jurídico, isso também fortalece a accountability, ou seja, a capacidade de identificar os responsáveis por ações tomadas em nome da segurança digital.

Por fim, é necessário consolidar marcos regulatórios internacionais que abordem os limites éticos da IA na cibersegurança. A ausência de padrões globais favorece a exploração de zonas cinzentas por governos autoritários e corporações sem compromisso com os direitos humanos. A ONU, por meio da Agenda Digital para o Desenvolvimento Sustentável (2020), já reconhece que a segurança cibernética deve respeitar princípios de transparência, equidade e dignidade humana. Essa diretriz precisa ser incorporada às políticas nacionais e aos códigos de conduta de empresas tecnológicas, para que a IA seja usada com responsabilidade e justiça.

5. A Cidadania Digital como Direito de Quarta Geração

O avanço da tecnologia e da interconectividade global exige uma atualização do próprio conceito de cidadania. Tradicionalmente associada a direitos civis, políticos e sociais — como o voto, a liberdade de expressão e o acesso à educação —, a cidadania precisa hoje incorporar um novo campo: o digital. Nesse contexto, propõe-se o reconhecimento da **cidadania digital como um direito de quarta geração**, alicerçado na garantia do acesso, da proteção, da privacidade e da autonomia dos indivíduos no ciberespaço. Esse novo paradigma exige uma atuação conjunta entre Estado, sociedade civil e empresas tecnológicas, para assegurar que os direitos fundamentais se mantenham válidos no ambiente virtual.

A cidadania digital não se limita ao uso de tecnologias ou à presença nas redes sociais. Ela envolve a capacidade de agir com consciência crítica no espaço digital, compreendendo as implicações de cada clique, curtida, compartilhamento ou dado fornecido. Para que essa consciência se concretize, é necessário que os indivíduos sejam formados não apenas como consumidores de tecnologia, mas como agentes digitais ativos, com habilidades de leitura crítica, segurança informacional e capacidade de atuação em redes. Isso implica não apenas alfabetização digital, mas também **educação para a autonomia digital**, especialmente entre populações historicamente excluídas da transformação tecnológica.

A digitalização de serviços públicos e a expansão de plataformas de participação online transformaram a internet em extensão do espaço público. Por isso, garantir direitos no ambiente digital significa também proteger a cidadania em sua plenitude. O acesso à internet, por exemplo, deve ser tratado como um direito básico, tal como água e eletricidade, pois é condição para o exercício de liberdades e deveres. Da mesma forma, o direito ao esquecimento, à

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

proteção contra a vigilância indiscriminada e à neutralidade da rede devem ser considerados **expressões contemporâneas da dignidade humana**.

Nesse cenário, a cidadania digital também passa a incorporar o direito à proteção contra abusos algorítmicos. A desigualdade informacional, que separa os que sabem ler e escrever algoritmos dos que apenas são por eles classificados, constitui um dos grandes desafios da democracia digital. A assimetria entre grandes corporações de tecnologia e usuários comuns exige regulamentação que proteja os mais vulneráveis. Nesse sentido, legislações como o **Marco Civil da Internet** (Brasil, 2014) e a **Lei Geral de Proteção de Dados Pessoais – LGPD** (Brasil, 2018) são marcos iniciais importantes, mas ainda insuficientes frente à complexidade e velocidade da inovação tecnológica.

A construção de uma cidadania digital plena implica também na inclusão de grupos tradicionalmente marginalizados no debate sobre tecnologia. Mulheres, pessoas negras, indígenas, pessoas com deficiência e comunidades periféricas devem ser protagonistas na definição das políticas digitais. Afinal, os algoritmos aprendem com dados do mundo real — e se esse mundo é desigual, as máquinas inevitavelmente replicarão essas distorções. Promover diversidade nos espaços de desenvolvimento e decisão tecnológica é, portanto, uma estratégia não apenas de justiça social, mas de melhoria ética e funcional dos sistemas digitais.

Por fim, reconhecer a cidadania digital como um direito de quarta geração é admitir que a fronteira entre o real e o virtual está cada vez mais tênue — e que a dignidade da pessoa humana precisa ser defendida em ambas as esferas. Essa perspectiva amplia o papel do cidadão contemporâneo, que agora deve ser educado, protegido e empoderado também no ciberespaço. A seção seguinte abordará, portanto, como políticas públicas podem institucionalizar essa visão, garantindo segurança digital de forma equitativa, sustentável e universal.

6. Políticas Públicas para a Segurança Digital Universal e Sustentável

A consolidação da segurança digital como direito universal e prática sustentável exige que os Estados assumam protagonismo no desenvolvimento de políticas públicas eficazes, inclusivas e tecnicamente adequadas. No entanto, o que se observa em grande parte dos países, especialmente no Sul Global, é a ausência de estratégias de longo prazo voltadas à proteção digital da população. A cibersegurança, quando tratada, costuma se restringir a ações pontuais, voltadas à proteção de instituições governamentais e setores estratégicos, deixando de lado o cidadão comum. Para que haja uma segurança digital democrática, é preciso ir além da defesa de infraestrutura: é necessário investir na construção de uma cultura de proteção digital cidadã.

Políticas públicas eficazes devem incluir, em primeiro lugar, a ampliação do acesso à internet segura e de qualidade. Não é possível falar em cibersegurança se milhões de pessoas ainda dependem de redes públicas instáveis ou de pacotes limitados, muitas vezes com restrições à navegação. A inclusão digital deve ser acompanhada da inclusão informacional — ou seja, garantir que todos tenham condições de compreender os riscos e direitos associados à sua presença online. Programas governamentais de capacitação, como cursos gratuitos de segurança digital básica, oficinas em comunidades e a inserção do tema nos currículos escolares, são ações que podem gerar impacto estrutural e duradouro.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Outro eixo fundamental é a regulação do ecossistema digital com base em princípios éticos e democráticos. A atuação de plataformas digitais, provedores de serviços e empresas de tecnologia deve ser regulada por marcos legais claros, que definam responsabilidades, limites e obrigações de transparência. A LGPD, no Brasil, e o GDPR, na União Europeia, são exemplos importantes, mas precisam ser acompanhados de fiscalização eficaz e capacidade institucional. Órgãos como Autoridades Nacionais de Proteção de Dados devem ser fortalecidos, tanto em estrutura quanto em independência, para que possam atuar com autonomia frente aos grandes interesses corporativos.

Adicionalmente, políticas públicas voltadas à segurança digital precisam contemplar estratégias de prevenção e resposta a incidentes. Isso inclui a criação de **Centros de Resposta a Incidentes Cibernéticos (CERTs)** com atuação nacional e regional, capazes de monitorar ameaças em tempo real, auxiliar instituições públicas e privadas e emitir alertas para a população. Também é fundamental a articulação com a sociedade civil organizada, universidades e empresas de tecnologia, criando ambientes colaborativos de inovação em cibersegurança. As políticas devem, ainda, considerar a sustentabilidade digital: garantir que os recursos tecnológicos utilizados para a segurança também respeitem critérios de eficiência energética e impacto ambiental reduzido.

A construção de uma segurança digital sustentável exige que essas ações não sejam episódicas ou dependentes de governos específicos, mas incorporadas como política de Estado. Planos nacionais de cibersegurança devem estabelecer metas plurianuais, recursos contínuos e mecanismos de avaliação de impacto. A segurança digital, assim como a educação ou a saúde, deve ser vista como um direito fundamental e um bem público, cuja garantia não pode ser terceirizada ou tratada como luxo tecnológico. Nesse sentido, a governança da segurança digital precisa ser participativa, permitindo que diferentes setores sociais tenham voz na definição de prioridades e estratégias.

Por fim, é necessário reconhecer que a segurança digital não é apenas um desafio nacional, mas uma questão global. A interdependência das redes e a transnacionalidade dos ataques exigem cooperação internacional. O fortalecimento de tratados multilaterais, o compartilhamento de boas práticas entre países e a criação de mecanismos globais de responsabilização são passos essenciais para uma cibersegurança verdadeiramente universal. A ONU, a União Internacional de Telecomunicações e fóruns como o IGF (Internet Governance Forum) já avançam nesse sentido, mas é preciso ampliar a representatividade e eficácia desses espaços. A soberania digital deve caminhar junto com a solidariedade digital, promovendo equidade, justiça e paz no ciberespaço.

7. Conclusão

A emergência da cibersegurança como questão central da vida contemporânea exige não apenas soluções técnicas, mas também abordagens éticas, políticas e educativas. Este artigo propôs uma análise aprofundada e inédita da cibersegurança sob a ótica da cidadania digital, da ética algorítmica e da autodefesa informacional, articulando campos distintos do saber — da ciência da computação ao direito, da filosofia da informação às políticas públicas. O conceito de **autodefesa digital algorítmica**, aqui desenvolvido, representa uma proposta de

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

enfrentamento crítico aos desafios da hipervigilância automatizada, colocando o sujeito como agente e não apenas como alvo dos sistemas digitais.

Conclui-se que a segurança digital não pode mais ser entendida como um serviço técnico prestado por terceiros ou como um bem de consumo de nicho. Ela deve ser tratada como um direito fundamental, expressão direta da dignidade humana no século XXI. Nesse sentido, a ampliação do acesso à informação, a criação de políticas públicas inclusivas e o fortalecimento das regulações algorítmicas tornam-se eixos indispensáveis para a proteção do indivíduo e da coletividade. O cidadão digital precisa ser alfabetizado não apenas para o uso, mas para a compreensão crítica e atuação consciente diante dos sistemas que o rodeiam.

A cidadania digital, proposta neste texto como um direito de quarta geração, requer reconhecimento institucional, investimento estatal e participação social. As desigualdades informacionais ampliam as vulnerabilidades e reproduzem lógicas históricas de exclusão e dominação. Por isso, o combate às assimetrias algorítmicas deve ser parte de um projeto maior de justiça informacional e soberania digital, que envolva os mais diversos setores sociais — especialmente aqueles que historicamente não foram incluídos nas decisões tecnológicas.

Além disso, a complexidade dos riscos contemporâneos exige uma governança global, capaz de harmonizar interesses nacionais com a universalidade dos direitos digitais. A criação de fóruns, tratados e órgãos internacionais de cibersegurança deve ser acompanhada por mecanismos efetivos de responsabilização e fiscalização, evitando que corporações transnacionais operem à margem da legalidade e da ética. A segurança cibernética não pode ser uma nova fronteira para o autoritarismo digital, mas um espaço de consolidação da democracia e da liberdade.

Em última instância, garantir segurança digital é garantir o direito de existir com dignidade no mundo conectado. Isso implica que cada indivíduo, ao acessar uma rede, enviar uma mensagem ou armazenar um dado, esteja protegido por sistemas transparentes, justos e sob controle social. A construção dessa realidade depende de escolhas políticas, educacionais e culturais, que começam no presente e moldarão o futuro. Cabe à sociedade contemporânea decidir se a era digital será marcada pela vigilância e pelo medo ou pelo conhecimento, pela justiça e pela liberdade informacional.

Referências

EUBANKS, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press, 2018.

EUROPEAN UNION. *General Data Protection Regulation (GDPR)*. Brussels: Official Journal of the European Union, 2016.

MARCO CIVIL DA INTERNET. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

MOROZOV, Evgeny. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs, 2013.

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

UNESCO. *Agenda Digital para o Desenvolvimento Sustentável: Segurança, Inclusão e Direitos Humanos no Ciberespaço*. Paris: UNESCO, 2020.

BRASIL. Lei n. 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.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.