***Review Article***

**Cybersecurity Gaps in Digital Epidemiology: Safeguarding Medical Surveillance in the Age of AI and Global Pandemics**

**Abstract**

Digital epidemiology leverages real-time data and artificial intelligence (AI) to monitor and predict disease trends. However, the expanding interface between public health surveillance and digital technology presents growing cybersecurity vulnerabilities. This review critically examines existing gaps in cybersecurity frameworks within digital epidemiology, focusing on the implications of AI-driven data analytics, regulatory shortcomings, and the disproportionate impact on low- and middle-income countries (LMICs). We propose a layered socio-technical framework to safeguard digital surveillance systems, integrating legal, ethical, and technological protections. Recommendations include privacy-preserving AI models, international legal harmonization, capacity building in LMICs, and ethical governance of public health surveillance.

**Keywords: Digital Epidemiology; Cybersecurity; Artificial Intelligence (AI); Health Data Privacy; Global Health Governance; Low- and Middle-Income Countries (LMICs)**

**1. Introduction**

The digital revolution has transformed nearly every sector of society, and public health is no exception. Digital epidemiology; defined as the use of digital data, tools, and platforms to understand and respond to health threats, has emerged as a critical pillar of modern disease surveillance [1]. From AI-powered outbreak prediction to mobile-based contact tracing, this field leverages vast data streams generated by individuals, institutions, and environmental sensors in real time [2]. Its importance became especially evident during global health emergencies such as the COVID-19 pandemic, when traditional surveillance methods proved too slow, fragmented, or resource-intensive to track fast-evolving outbreaks [3].

However, the promise of digital epidemiology comes with significant risks—most notably, vulnerabilities in cybersecurity. As health systems become increasingly digitized, they are exposed to a growing array of cyber threats, including data breaches, model manipulation, and targeted misinformation campaigns [4, 5]. The integration of artificial intelligence (AI), while offering unprecedented speed and predictive power, complicates security further. AI systems are often opaque, susceptible to adversarial inputs, and difficult to audit for bias or fairness [6]. These challenges raise concerns not only about technical failures but also about trust, equity, and harm in vulnerable populations.

The implications of cybersecurity failures in digital health systems extend far beyond privacy violations. Compromised surveillance systems can lead to misdiagnoses, stigmatization, public panic, and delayed or misguided interventions [7]. For instance, manipulated health data may distort epidemiological models, while leaked vaccination records may fuel disinformation or discrimination. In many low- and middle-income countries (LMICs), where digital literacy is low and cybersecurity infrastructure is weak, these threats are magnified [8]. Despite this, cybersecurity is often treated as an afterthought in global health strategy, policy design, and funding allocation.

Moreover, because pathogens and digital systems do not respect borders, the risks of cyber-insecure digital epidemiology are global. Weak links in one nation’s surveillance network can enable the spread of misinformation or malware across regions, undermining global public health efforts. This interconnectedness demands a harmonized, multi-layered approach to cybersecurity; one that integrates technical protections, human-centered safeguards, ethical principles, and international governance mechanisms [9].

This review addresses these challenges through a socio-technical systems framework that unites insights from public health, cybersecurity, artificial intelligence, and global governance. It classifies and contextualizes the key cybersecurity threats to digital epidemiology, analyzes real-world case studies, and proposes a layered security model for building resilient systems. Special attention is given to global disparities, with a focus on LMIC vulnerabilities and the need for inclusive, globally coordinated responses.

In the age of AI and pandemics, the success of digital epidemiology hinges on its security. Without strong and ethical cybersecurity foundations, the same tools designed to protect public health may inadvertently endanger it.

## **1.2. Conceptual Framework: A Socio-Technical Lens on Cybersecurity in Digital Epidemiology**

## To anchor our analysis, we adopt a **socio-technical systems theory** framework. This approach recognizes that technological tools (e.g., AI, databases, mobile apps) are deeply embedded within social, legal, and organizational contexts. Effective cybersecurity requires concurrent alignment across:

* **Technical layers** (data encryption, AI safety, software auditing),
* **Human layers** (training, awareness, ethical practices), and
* **Institutional layers** (regulation, oversight, governance).

This framework enables a layered analysis of cybersecurity vulnerabilities across the digital epidemiology lifecycle: data collection, transmission, analysis, dissemination, and feedback.

**2. Cybersecurity Landscape in Digital Epidemiology**

**2.1 Data Sources and Digital Infrastructure**

Digital epidemiology thrives on the integration of high-volume, high-velocity, and high-variety data. These inputs span across multiple domains: clinical data from **electronic health records (EHRs)**, biometric readings from **wearable sensors**, behavioral insights from **mobile health (mHealth) apps**, textual and multimedia content from **social media platforms, genomic databases, and crowd-sourced reports** from community health applications [10, 11]. These datasets, when fused and analyzed using **AI algorithms and machine learning models**, enable real-time disease surveillance, outbreak prediction, and resource allocation.

However, this **multi-source integration** creates a highly heterogeneous and distributed digital ecosystem. Many of these systems are hosted across **cloud-based infrastructures, edge computing environments,** and **Internet-of-Things (IoT)** devices that communicate across dynamic, and often loosely regulated, networks [12]. For instance, wearable devices may continuously transmit health signals to cloud dashboards through third-party APIs, while mobile apps may upload user-generated symptom data to centralized repositories or AI models for processing.

Such **heterogeneity and interconnectivity** introduce major cybersecurity risks. Each layer of the data pipeline from **collection at the device level**, to **transmission via network protocols**, to **storage in cloud-based servers**, and **AI-based analysis** is a potential attack vector. **Vulnerabilities in APIs, unsecured device firmware, poorly encrypted data transmissions**, or **inadequate authentication mechanisms** can expose sensitive health data to unauthorized access, manipulation, or exploitation [13].

Moreover, the **high-speed nature of real-time digital surveillance** reduces the margin for error. A single breach or manipulation; such as tampering with input data streams or injecting adversarial examples into AI models can rapidly cascade into flawed epidemiological predictions or inappropriate public health responses. This is particularly concerning in pandemic contexts, where such errors may result in misallocation of resources, erosion of public trust, or preventable morbidity and mortality [14].

Additionally, **data sovereignty and jurisdictional ambiguity** complicate the cybersecurity landscape. Many digital epidemiology platforms are developed or hosted by multinational tech firms, leading to cross-border data transfers that may not be protected by local privacy laws; especially in low- and middle-income countries (LMICs), where regulatory frameworks may be outdated or underdeveloped [15]. As such, not only are the **technical systems** vulnerable, but the **governance structures** around them may also lack the capacity to detect, respond to, or mitigate cyber incidents effectively.

In summary, while digital infrastructure enables unprecedented capabilities in public health intelligence, it also vastly enlarges the **attack surface** for malicious actors. A robust cybersecurity strategy must therefore account for this **complex and layered architecture**, including both technological and institutional safeguards, to ensure system resilience and public trust.

### **1.5. Types of Cybersecurity Threats**

### Cybersecurity threats to digital epidemiology systems are increasingly complex and multidimensional, arising from the convergence of sensitive health data, real-time surveillance, and advanced computational tools such as artificial intelligence (AI). These threats compromise the confidentiality, integrity, and availability (CIA triad) of digital public health infrastructures, with far-reaching consequences for both individuals and populations. The most prominent categories of threats include:

### **1.5.1 Data Breaches and Ransomware Attacks**

### Health surveillance systems are frequent targets of data breaches due to the high value of medical information on the dark web. Electronic health records (EHRs), in particular, contain sensitive identifiers such as biometrics, medical histories, and insurance details, which can be exploited for identity theft, insurance fraud, or social engineering attacks [16]. In ransomware scenarios, attackers gain control of surveillance databases or public health dashboards and demand payment to restore access; paralyzing outbreak monitoring, delaying vaccine distribution, or stalling emergency responses [17].

### Example: In 2021, Ireland’s national health service experienced a major ransomware attack that shut down several public health systems, severely affecting patient care and COVID-19 data reporting [18].

### **1.5.2 AI Manipulation and Adversarial Attacks**

### As AI models become integral to digital epidemiology used for case prediction, hotspot mapping, and risk stratification—they become potential targets for adversarial threats. **Data poisoning attacks** inject corrupted training data to skew model outputs, while **adversarial examples** use subtle input modifications to mislead AI classification [19]. Furthermore, **model inversion attacks** can reverse-engineer AI outputs to reconstruct sensitive data about individuals in training datasets [20]. These threats undermine model integrity, bias public health decisions, and erode trust in automated surveillance tools.

### **Risk:** Misclassified outbreaks or falsely predicted disease clusters could redirect public health resources away from actual hotspots, resulting in delayed interventions and higher mortality.

**1.5.3 Surveillance Overreach and Civil Liberties Erosion**

In the name of emergency preparedness, governments may deploy digital surveillance technologies such as contact-tracing apps or geolocation trackers without adequate checks and balances. This raises concerns of **mission creep**, where systems designed for epidemiology are later repurposed for political surveillance or law enforcement [21]. Unauthorized access by third parties, or inadequate anonymization of datasets, may violate privacy rights and chill public participation in health programs, particularly in politically repressive contexts.

**Ethical concern:** During the COVID-19 pandemic, several countries expanded digital surveillance tools without sunset clauses or oversight mechanisms, sparking debates about privacy versus public safety [22].

**1.5.4 Disinformation and Data Corruption**

Epidemiological data systems are vulnerable to **information warfare**, where state or non-state actors inject false or misleading data to manipulate public perception or disrupt response coordination. Automated bots can generate **false symptom reports**, skew sentiment analyses on social media, or inject disinformation into dashboards via open reporting interfaces [23]. These activities can trigger public panic, erode trust in health authorities, and distort predictive models used to allocate medical resources.

**Case in point:** Coordinated misinformation campaigns on social media during COVID-19 led to vaccine hesitancy, mask refusal, and violent protests; highlighting the direct health consequences of digital disinformation.

**Table 1. Key Data Sources and Associated Cybersecurity Vulnerabilities**

|  |  |  |  |
| --- | --- | --- | --- |
| ****Data Source**** | ****Technology Used**** | ****Vulnerability**** | ****Potential Impact**** |
| Electronic Health Records | Cloud-based storage | Data breach, unauthorized access | Loss of sensitive health information |
| Wearables & Mobile Apps | Bluetooth, GPS | Device spoofing, location tracking | Behavioral profiling, privacy invasion |
| Genomic Databases | Cloud / Genomic AI | Bioterrorism, data misuse | Genetic discrimination, potential weaponization |
| Social Media Feeds | NLP, sentiment analysis | Data poisoning, misinformation injection | Skewed surveillance data, delayed response |

1. EHRs are highly sought after by cybercriminals due to their resale value on the black market [24].
2. Many wearable devices transmit unencrypted data over public networks, making them susceptible to spoofing and unauthorized tracking [25].
3. Genomic data are immutable and uniquely identifiable, posing risks of long-term re-identification or misuse in synthetic biology [26].
4. Social media platforms are prone to coordinated manipulation by bots and trolls, which can distort public health sentiment analyses [27].

**1.6. Case Studies: Lessons from Global Pandemics**

**Table 2: Cybersecurity Concerns in COVID-19 Digital Surveillance Tools**

|  |  |  |  |
| --- | --- | --- | --- |
| Country | Tool/Platform | Security Issue Identified | Consequence/Response |
| Singapore | TraceTogether | Bluetooth spoofing, centralized database | Limited adoption, policy reform |
| UK | NHS COVID-19 App | Risk of deanonymization | Public concern, transparency updates |
| Global | GISAID, Nextstrain | Lack of unified security protocols | Potential espionage, uneven global access |
| USA | Johns Hopkins Dashboard | Misinformation bots, phishing clones | Public confusion, cybersecurity tightening |

1. TraceTogether's repurposing of data for police use caused backlash [28].
2. NHS app faced criticism over potential re-identification [29].
3. GISAID’s access policies raised concerns about fairness and data sovereignty [30].
4. The Johns Hopkins dashboard was cloned for malware distribution [31].

**1.7 COVID-19 and Contact Tracing Apps** Countries such as Singapore (TraceTogether), the UK (NHS COVID-19), and Australia (COVID Safe) deployed contact tracing apps. However, many faced criticism for weak encryption, insufficient anonymization, and inadequate transparency. Data centralization increased the risk of breaches, and uptake was hindered by privacy concerns.

**1.8 Genomic Surveillance and International Platforms** Global platforms like GISAID and Nextstrain facilitated SARS-CoV-2 variant tracking but raised concerns about data ownership, potential bioterrorism risks, and geopolitical misuse [31]. Inconsistent security standards across contributors heightened exposure to cyber espionage.

**1.9 Misinformation and Dashboard Manipulation** Real-time dashboards by organizations like Johns Hopkins were targets of misinformation campaigns and bot-driven disinformation, leading to public confusion and erosion of trust in data [33, 34].

**1.10. Gaps in Regulatory and Ethical Frameworks**

**Table 3: Comparative Overview of Legal Frameworks and Their Limitations**

|  |  |  |  |
| --- | --- | --- | --- |
| Framework | Scope | Cybersecurity Gaps | Relevance to Digital Epidemiology |
| HIPAA (USA) | Patient data privacy | No AI model audit provisions | Limited to U.S. healthcare settings |
| GDPR (EU) | General data protection | Consent in AI/IoT, cross-border enforcement unclear | Passive data tracking still problematic |
| IHR (WHO) | International health regulations | No mention of digital tools, cybersecurity specifics | Outdated for modern epidemiological tools |

1. HIPAA lacks requirements for algorithmic transparency in AI systems [35].
2. GDPR struggles with enforcing AI accountability across borders [36].
3. IHR’s current version does not address cybersecurity or digital tools [37].

While laws like the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) offer foundational protections, they fall short in addressing AI-specific and transnational cybersecurity risks. Current frameworks:

* Do not mandate security audits of AI models used in epidemiology.
* Lack provisions for algorithmic transparency and explainability.
* Struggle to address consent in passive data collection (e.g., location tracking).
* Do not enforce standards for cross-border data governance or accountability in collaborative platforms.

Ethical gaps include data sovereignty violations, surveillance without democratic oversight, and inequitable access to secure technology in low-resource settings [38].

**1.11. Bridging the Gaps: Strategies for Cybersecure Epidemiology**

**Table 4: Emerging Technologies and Their Relevance to Secure Epidemiology**

|  |  |  |  |
| --- | --- | --- | --- |
| Technology | Function | Strength | Limitation |
| Differential Privacy | Adds statistical noise to datasets | High anonymity, scalable | May reduce data accuracy |
| Federated Learning | Model training without raw data sharing | Privacy-respecting, distributed learning | Complex implementation, slower convergence |
| Homomorphic Encryption | Data processing without decryption | High confidentiality | Computation-intensive |
| AI Red-teaming | Adversarial testing of AI systems | Exposes system vulnerabilities proactively | Requires expertise and resources |

1. Differential privacy is used by the U.S. Census and Apple [21].
2. Federated learning reduces data exposure by training models locally [22].
3. Homomorphic encryption allows secure computation but is resource-heavy [22].
4. AI red-teaming helps identify exploitable flaws before deployment [23].

**1.12. Privacy-Preserving Technologies**

**Table 5: Strategic Recommendations for Future Research and Policy**

|  |  |  |
| --- | --- | --- |
| Focus Area | Proposed Action | Expected Outcome |
| Cybersecurity simulation labs | Stress-test AI surveillance tools against cyberattacks | Robust model defense, increased trustworthiness |
| AI ethics certification | Develop global certification frameworks | Standardized, safe deployment of digital tools |
| Capacity building in LMICs | Train public health professionals in cybersecurity principles | Narrowing digital equity and skills gap |
| Interdisciplinary collaboration | Joint programs in public health, CS, and law | Holistic and sustainable policy development |

1. Cyberattack simulations improve preparedness and system resilience [24].
2. Certification efforts are aligned with emerging AI regulation frameworks [25].
3. Capacity building in LMICs is crucial to global health security [26].
4. Interdisciplinary integration ensures ethical and practical relevance [27].

Techniques like federated learning, differential privacy, and homomorphic encryption can allow data analysis without compromising personal information. These methods enable collaborative surveillance while minimizing data exposure.

**2.1 AI Transparency and Auditability**

Developing explainable AI models and establishing routine audits of algorithmic outputs are essential to detect manipulation and ensure public trust. Model documentation and third-party validation should become standard practice.

**2.2. Cross-Sector Collaboration**

Cybersecurity in digital epidemiology requires partnerships between public health institutions, cybersecurity experts, and private tech companies. Establishing a global task force, potentially under WHO, could facilitate coordination and response to cyber threats.

**2.3. Legal and Policy Reforms**

New international agreements akin to the International Health Regulations (IHR) should be developed to govern digital health cybersecurity [27]. These should address cross-border data sharing, AI accountability, and emergency protocols for cyber incidents during pandemics.

**3.1 Future Directions**

Future research should focus on dynamic risk modeling for epidemiological platforms, AI ethics certification, and training programs to enhance cybersecurity literacy among public health professionals. Simulation tools for cyberattack scenarios could also prepare systems for real-world challenges. Establishing cyber-resilience benchmarks for health surveillance technologies will be pivotal in ensuring sustainable and secure digital epidemiology.

**4. Conclusion**

Digital epidemiology stands at the intersection of opportunity and vulnerability. While AI and big data enhance our ability to detect and respond to health crises, they also expose public health systems to unprecedented cybersecurity risks. Addressing these gaps requires a multidimensional approach technical, legal, and ethical. Without urgent reforms, the trust and efficacy of digital epidemiological tools will remain fragile, threatening the global capacity to combat future pandemics.

**References**

1. Asi, Y. M., & Williams, C. (2018). The role of digital health in making progress toward Sustainable Development Goal (SDG) 3 in conflict-affected populations. *International Journal of Medical Informatics*, 114, 114–120. <https://doi.org/10.1016/j.ijmedinf.2017.11.003>
2. Brundage, M., Avin, S., Clark, J., et al. (2020). Toward trustworthy AI development: Mechanisms for supporting verifiable claims. *arXiv preprint*, arXiv:2004.07213.
3. Dong, E., Du, H., & Gardner, L. (2020). An interactive web-based dashboard to track COVID-19 in real time. *The Lancet Infectious Diseases*, 20(5), 533–534. [https://doi.org/10.1016/S1473-3099(20)30120-1](https://doi.org/10.1016/S1473-3099%2820%2930120-1)
4. Gostin, L. O., Cohen, I. G., & Koplan, J. P. (2020). Universal health coverage and the pandemic treaty: Governance and equity in global health security. *JAMA*, 326(13), 1253–1254.
5. Lazer, D., Kennedy, R., King, G., & Vespignani, A. (2014). The parable of Google Flu: Traps in big data analysis. *Science*, 343(6176), 1203–1205. <https://doi.org/10.1126/science.1248506>
6. Radanliev, P., De Roure, D., Walton, R., et al. (2020). Artificial intelligence and big data in cybersecurity: Emerging threats and countermeasures. *Journal of Cybersecurity Technology*, 4(1), 1–14. <https://doi.org/10.1080/23742917.2020.1728258>
7. Salathé, M., Bengtsson, L., Bodnar, T. J., et al. (2012). Digital epidemiology. *PLOS Computational Biology*, 8(7), e1002616. <https://doi.org/10.1371/journal.pcbi.1002616>
8. Tiffin, N. (2020). Health data governance: Are we making progress in the African region? *Global Health Action*, 13(1), 1804036. <https://doi.org/10.1080/16549716.2020.1804036>
9. Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. *PLOS Medicine*, 15(11), e1002689. <https://doi.org/10.1371/journal.pmed.1002689>
10. Brundage, M., Avin, S., Clark, J., et al. (2020). Toward trustworthy AI development: Mechanisms for supporting verifiable claims. *arXiv preprint*, arXiv:2004.07213.
11. Dong, E., Du, H., & Gardner, L. (2020). An interactive web-based dashboard to track COVID-19 in real time. *The Lancet Infectious Diseases*, 20(5), 533–534. [https://doi.org/10.1016/S1473-3099(20)30120-1](https://doi.org/10.1016/S1473-3099%2820%2930120-1)
12. Radanliev, P., De Roure, D., Walton, R., et al. (2020). Artificial intelligence and big data in cybersecurity: Emerging threats and countermeasures. *Journal of Cybersecurity Technology*, 4(1), 1–14. <https://doi.org/10.1080/23742917.2020.1728258>
13. Salathé, M., Bengtsson, L., Bodnar, T. J., et al. (2012). Digital epidemiology. *PLOS Computational Biology*, 8(7), e1002616. <https://doi.org/10.1371/journal.pcbi.1002616>
14. Tiffin, N. (2020). Health data governance: Are we making progress in the African region? *Global Health Action*, 13(1), 1804036. <https://doi.org/10.1080/16549716.2020.1804036>
15. Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. *PLOS Medicine*, 15(11), e1002689. <https://doi.org/10.1371/journal.pmed.1002689>
16. Cho, H., Ippolito, D., & Yu, Y. W. (2020). Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. arXiv preprint arXiv:2003.11511.
17. Cyranoski, D. (2020). South Korea is reporting intimate details of COVID-19 cases: Has it helped? Nature, 581(7809), 19. <https://doi.org/10.1038/d41586-020-01090-7>
18. Ekong, I., Chukwu, E., & Chukwu, M. (2020). COVID-19 mobile positioning data contact tracing and patient privacy regulations: The Nigerian context. Frontiers in Communications and Networks, 1, 1–7. <https://doi.org/10.3389/frcmn.2020.00002>
19. European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union, L119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
20. Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020). Digital tools against COVID-19: Framing the ethical challenges and how to address them. JMIR mHealth and uHealth, 8(7), e8954. <https://doi.org/10.2196/8954>
21. Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. Nature Medicine, 26, 463–464. <https://doi.org/10.1038/s41591-020-0832-5>
22. Lepri, B., Oliver, N., Letouzé, E., Pentland, A., & Vinck, P. (2018). Fair, transparent, and accountable algorithmic decision-making processes: The premise, the proposed solutions, and the open challenges. Philosophy & Technology, 31(4), 611–627. <https://doi.org/10.1007/s13347-017-0279-x>
23. Marcus, G. (2022). The next decade in AI: Four steps towards robust artificial intelligence. Communications of the ACM, 65(2), 26–28. <https://doi.org/10.1145/3505633>
24. Mooney, S. J., Pejaver, V., & Vardhan, M. (2021). Federated learning for epidemiology: Opportunities and challenges. American Journal of Epidemiology, 190(12), 2594–2601. <https://doi.org/10.1093/aje/kwab158>
25. OECD. (2019). Recommendation of the Council on Artificial Intelligence. Organisation for Economic Co-operation and Development. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
26. Park, S., Choi, G. J., & Ko, H. (2020). Information technology–based tracing strategy in response to COVID-19 in South Korea—Privacy controversies. JAMA, 323(21), 2129–2130. <https://doi.org/10.1001/jama.2020.6602>
27. Raji, I. D., Binns, R., Veale, M., Van Kleek, M., & Shadbolt, N. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT), 33–44. <https://doi.org/10.1145/3351095.3372873>
28. Rocher, L., Hendrickx, J. M., & de Montjoye, Y. A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. Nature Communications, 10, 3069. <https://doi.org/10.1038/s41467-019-10933-3>
29. Sharma, T., Bashir, M., & Zimmer, M. (2020). Public trust in contact-tracing apps: A study on Ghana’s COVID-19 response. Information, Communication & Society. <https://doi.org/10.1080/1369118X.2020.1835225>
30. Suresh, H., & Guttag, J. V. (2021). A framework for understanding unintended consequences of machine learning. Communications of the ACM, 64(4), 62–71. <https://doi.org/10.1145/3436251>
31. Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. Northwestern Journal of Technology and Intellectual Property, 11(5), 239–273. <https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1>
32. WHO. (2022). Digital Health Guidelines: A Global Strategy on Digital Health 2020–2025. World Health Organization. <https://www.who.int/publications/i/item/9789240020924>
33. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
34. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 317–331. <https://doi.org/10.1016/j.patcog.2018.07.023>
35. Broniatowski, D. A., Jamison, A. M., Qi, S. H., et al. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American Journal of Public Health*, 108(10), 1378–1384. <https://doi.org/10.2105/AJPH.2018.304567>
36. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas*, 113, 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>
37. Erlich, Y., & Narayanan, A. (2014). Routes for breaching and protecting genetic privacy. *Nature Reviews Genetics*, 15(6), 409–421. <https://doi.org/10.1038/nrg3723>
38. Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1322–1333).