Cybersecurity Imperatives for Fashion Tech: A DPDP Act, 2023 Compliance Analysis in Wearable Technology and Smart Clothing

Profile of the Author:

Designation: 3rd Year B.A. L.L.B. (Hons.) Student at School of Law, CHRIST (Deemed to be University), Bangalore

Email ID: aishah.afreen@law.christuniversity.in

Contact: +91 97413 98073

Official Address: 'Misbah', Coelho Lane, Falnir Road, Mangalore – 575001.

Cybersecurity Imperatives for Fashion Tech: A DPDP Act, 2023 Compliance Analysis in Wearable Technology and Smart Clothing

-Aishah Afreen Misbah[1]

Abstract

The digital revolution in the fashion industry has given rise to a transformative era with wearable technology and smart clothing taking center stage. The paper delves into the intersection of fashion and technology, specifically exploring the cybersecurity and data privacy concerns surrounding wearable technology and smart clothing. Wearable technology has evolved from simple fitness trackers to sophisticated accessories such as smart-watches and smart-glasses. Unlike traditional clothing, smart clothing uses digital components such as an electronic chip, sensor, and battery that can be integrated into conductive fibres. While these innovations offer exciting possibilities, they also raise significant cybersecurity challenges such as device hacking, wireless communication risks, the collection and transmission of sensitive data, including biometrics, location, and health information, thus exposing users to potential privacy breaches. With the advent of Digital Personal Data Protection Act, 2023 in the Indian legal framework, this paper evaluates the applicability and effectiveness of the regulation in mitigating the cybersecurity and data privacy issues in wearable devices. Through stringent security measures, breach reporting, and robust consent regulations, the act aligns with global privacy standards, providing a framework to secure user data and promote responsible innovation in the digital fashion realm. By examining the DPDP Act, this paper illustrates its potential impact and highlights its alignment with international privacy regulations and the need for a balanced approach that fosters innovation while safeguarding the fundamental rights of individuals in the digital age.

Keywords: Cyber Security, Data Breach, Smart Fashion, Transparency, Wearable Devices

[1] Author is a 3rd Year B.A. L.L.B. (Hons.) Student at School of Law, CHRIST (Deemed to be University), Bangalore. She can be contacted at aishah.afreen@law.christuniversity.in.

I. Introduction

The fashion industry, which has historically been famed for its artistry and innovation, has enthusiastically embraced the digital revolution. Technology has effortlessly woven itself into the fabric of fashion. This digital shift has not only changed the way fashion is produced and consumed, but it has also ushered in a new era of opportunities marked by the union of fashion and technology. The fast emergence of wearable technology in fashion is at the heart of this revolution. Wearables, which were originally limited to fitness trackers and smartwatches, have evolved beyond their practical roots to become a fashion statement in their own right. Smart clothes, intelligent accessories, and even tech-infused materials have found their way onto fashion runways and into customers' everyday wardrobes. Several recent field research and business publications predicted that the wearable technology market will have a significant influence and irreversible expansion, especially in the fashion industry. These research predicted a $231 billion wearables industry by 2032 and a strong presence of wearable technology in digital society, with many applications in retail, automobile, medical, and insurance.[2] There is a distinction between products intended primarily for industrial, medicinal, and other utilitarian uses and those intended primarily for consumer use. Wearable devices have great potential medicinal and industrial uses. Nonetheless, the prospective consumer market has sparked the most interest in the financial press.[3]

However, the merging of fashion and technology is not without its difficulties. Wearables are becoming vulnerable targets for cyber-attacks since they capture and send a wealth of personal data ranging from biometrics to health measurements. This brings us to a critical point: the importance of cybersecurity and data privacy at the fashion-tech confluence. As people use smart clothes and accessories that track their every move and physiological detail, safeguarding their data becomes increasingly important. The fashion business must be concerned not just with aesthetics, but also with the security of its customers' most private digital selves. Despite the significant engagement, consumers are rarely aware of when and what data is shared on the internet by their smart gadgets, and are utterly oblivious that their data is routinely kept and

---

[2] *Wearable Technology Market Worth Over USD 231 Billion by 2032, At CAGR 14.60%,* GLOBE NEWS WIRE (Aug. 31, 2023, 10:28 PM), https://www.globenewswire.com/en/news-release/2023/03/13/2626170/0/en/Wearable-Technology-Market-Worth-Over-USD-231-Billion-by-2032-At-CAGR-14-60.html

[3] Jeanne L. Schroeder, *Technology, Gender and Fashion*, 34 CARDOZO Arts & ENT. L.J. 754, 764-765 (2016), https://www.cardozoaelj.com/wp-content/uploads/2016/08/SCHROEDER-ARTICLE.pdf

resold.[4] As the number of IoT players rises, so does the relevance of data laws, regulations, and policies.[5] The Digital Personal Data Protection Act of 2023[6] (DPDP Act) is one such advancement. This forward-thinking legislation is likely to transform the landscape of data privacy and cybersecurity by establishing strong data protection rules.

Thus, the objective of this paper is to assess the current landscape of cybersecurity and data privacy challenges in wearable technology within the fashion industry, identifying key vulnerabilities, data collection practices, and potential threats to user privacy. It further aims to analyse the impact of the Digital Personal Data Protection Act, 2023, on data protection and cybersecurity measures in the fashion-tech sector, and to evaluate how well these measures align with international privacy regulations, aiming to provide recommendations for improved data security and privacy in wearable technology.

II. Wearable Tech and Smart Clothing in Fashion

Wearable technology refers to any electronic equipment that is meant to be worn on the user's body. The wearables have sensors and other electronic components that often send data to the apps and give people trackable metrics or additional helpful information.[7] Such gadgets can take several forms, including accessories, medical equipment, and garments or clothing elements. Most wearable devices are accessories like smartwatches, smart glasses and fitness trackers. Artificial intelligence (AI) hearing aids, Google Glass, Microsoft's HoloLens, and a holographic virtual reality (VR) headset are among the most advanced instances of wearable technology.[8]

On the other hand, smart clothes have electronics sewn directly into the fabrics. Traditional textiles and fibres are integrated with electronics to capture and send data and information about heat, light, movement, and other environmental factors using electronic sensors.[9] Various

---

[4] Irene Ioannidou and Nicolas Sklavos, *On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications*, 5 CRYPTOGRAPHY. 29, 29 (2021). https://www.mdpi.com/2410-387X/5/4/29

[5] Suada Hadzovic, Sasa Mrdovic and Milutin Radonjic, *Identification of IoT Actors*, 21 SENSORS, (2021). https://www.mdpi.com/1424-8220/21/6/2093

[6] The Digital Personal Data protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

[7] Robin Wright and Latrina Keith, W*earable Technology: If the Tech Fits, Wear It,* 11 JOURNAL OF ELECTRONIC RESOURCES IN MEDICAL LIBRARIES 204, 205 (2014).

[8] *Ibid.*

[9] B. Ariyatum, R. Holland, D. Harrison and T. Kazi, *The future design direction of Smart Clothing development,* 96 THE JOURNAL OF THE TEXTILE INSTITUTE 199, 201 (2010)

fashion brands and tech companies are pioneering smart clothing and wearables. Pizza Hut's smart shoes allow pizza orders, Nike's Adapt Shoes monitor workout data, and Under Armour's Athlete Recovery Sleepwear enhances sleep quality. Samsung offers a smart suit for digital interactions and the Body Compass workout shirt for biometric monitoring. Additionally, Samsung caters to golfers with weather-adaptive apparel. These innovations showcase the fusion of fashion and tech in wearable products that offer unique functionalities and experiences to consumers. While this is carving out a market position for itself in the consumer sector, a troubling problem is that the majority of customers are either unaware of the cybersecurity threats[10] posed by these wearables or have serious misunderstandings regarding privacy in relation to these devices.

III. Cybersecurity and Data Protection in the DPDP Era

Information devices, such as PCs, laptops, tablets, and smartphones, have been subject to security risks throughout their brief history. If the device is hacked, the data stored on or via it might be destroyed, stolen, or modified, resulting in severe implications.[11] Wearables are perhaps the most personal and intimate IT devices available, promising huge benefits for both individuals and the fashion industry. However, because they are more personal and intimate, their security is much more important. Keeping wearable gadgets and highly personal data secure presents significant hurdles.

Cybersecurity in the context of wearable devices has received much attention. Internet-connected sensors, equipment, and networks are routinely the targets of hacks, extortion, theft, and even destruction. Because an IoT-based smart grid may have millions of internet nodes distributed across enormous geographical regions, it is the most vulnerable to major assaults. A cyber-attack on wearables thus has horrible effects and tremendous financial harm as it includes the users' critical personal data.[12] This vulnerability can allow hackers to compromise smartphones and access other organizational resources, potentially exposing sensitive data. For instance, fitness trackers can divulge extensive user information, including activity patterns,

---

[10] L. Hagen, *"Overcoming the privacy challenges of wearable devices: A study on the role of digital literacy,"* in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 598–599. http://doi.acm.org/10.1145/3085228.3085254

[11] Adam J. Mills, Richard T. Watson, Leyland Pitt, and Jan Kietzmann, *Wearing safe: Physical and informational security in the age of the wearable device*, 59 BUSINESS HORIZONS 615, 615 (2016).

[12] K. Kimani, V. Oduol, and K. Langat, *Cyber security challenges for IoT-based smart grid networks,* 25 INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 36, 37 (2019) https://doi.org/10.1016/j.ijcip.2019.01.001

locations, demographics, and more.[13] While some may consider this data innocuous, it holds value for certain companies and marketers. Other, more permanent and crucial data, such as the wearer's date of birth and social security number, can also be retrieved via wearables. Personal information like this is far of greater worth than a stolen credit card number on the black market.[14] Hackers could exploit this information, selling it to third parties for various purposes, such as targeted marketing. Therefore, the security of wearable device connections to corporate networks is of paramount concern.

Major data breaches at companies like Target and Sony garnered widespread attention, causing nightmares for countless individuals dealing with identity theft. Even technologies not typically associated with IT displayed vulnerabilities. Concerned parents discovered that their baby monitors could be accessed by outsiders, and hackers managed to halt a Jeep Cherokee on a highway by remotely compromising its control systems.[15] Thus, a fundamental principle in cybersecurity is that industries must safeguard their data's confidentiality, availability, and integrity (referred to as security objectives) throughout its transmission, processing, and storage phases (referred to as data states). This protection is achieved by employing the right technology, policies, and personnel (referred to as countermeasures).[16]

Thus, the paramount concern surrounding wearables revolves around privacy, a cherished value that has attained the status of a fundamental right under Article 21[17] and must be upheld. In India, notable legal judgments on the right to privacy, such as *K.S. Puttaswamy v. Union of India*[18] have emerged. This precedent underscored the urgency and importance of data privacy, ultimately leading to the enactment of the Digital Personal Data Protection Act of 2023 (DPDP Act). This legislation, inspired by the European Union's emphasis on privacy and data protection, reflects India's commitment to aligning its policies with global standards. Like the GDPR[19], the DPDP Act signifies a pivotal shift towards stringent data protection measures. The significance of DPDP is that it applies to all companies and entities established within India that process personal data as part of their operations, regardless of where the data is

---

[13] Mohammed Saleh and Issam T. Hamdan, *Analysis on Security Vulnerabilities of Medical Wearable Devices (Fitness Trackers)*, 2 ENG. WORLD OPEN ACCESS JOURNAL 162, 163 (2020).
[14] Maggie Overfelt, The price of the wearable craze: Less data security, NBC NEWS (Sep. 03, 2023, 7:29 PM), https://www.nbcnews.com/tech/innovation/price-wearablecraze-less-data-security-n479271
[15] *Supra* note 10.
[16] *Ibid.*
[17] INDIA CONST. art. 21
[18] K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1
[19] General Data Protection Regulation, 2016, No. 679, Acts of European Parliament, (EU)

processed as well as to any companies established outside the country, monitoring the individual users' behaviour in India.

The DPDP Act establishes measures to guarantee that when a corporation gathers personal data from an individual, it does so in a fair, lawful, and secure manner. Fundamentally, a business must have a proper legal basis for collecting or utilising data (i.e. processing). The statute establishes three legal basis, which are as follows: consent from the person[20]; that the processing is required for the performance of a contract with the individual; and that the processing is required to meet a statutory obligation[21]. Furthermore, the firm processing the personal data must have informed the individual concerned about how and why their information is being processed.[22] Personal data acquired by a wearable device, in the wrong hands, might provide an alarming glimpse into the user's health, habits, whereabouts, and activities. Companies that process personal data have to be explicit about the objective of their processing from the start. Care is additionally needed to ensure that the data fiduciary does not process more personal data than is required and that personal data is only handled for the duration required to accomplish the purpose.[23] If new uses for the data are necessary, a legal justification for such processing must be found and informed to data principals.

Central to all these elements is the overarching concept of accountability. This entails that the entire system should be structured with a primary focus on proactively safeguarding data, both in design and as a default setting, and all of these measures must be verifiable. In the context of wearable technology and smart clothing, the starting point aligns with the notion of 'accountability,' a novel security approach mandated by the DPDP Act to govern corporate operations and personal data handling with a robust data protection perspective. In practical terms, across these three domains, accountability is attained through a set of responsibilities, by designating a Consent Manager[24] and a Data Protection Board.[25]

---

[20]The Digital Personal Data protection Act, 2023, § 6, No. 22, Acts of Parliament, 2023 (India).
[21] The Digital Personal Data protection Act, 2023, § 7, No. 22, Acts of Parliament, 2023 (India).
[22] The Digital Personal Data protection Act, 2023, § 4, No. 22, Acts of Parliament, 2023 (India).
[23] Joanne Vengadesan and Katie Gordon, GDPR In Sport, PENNINGTONS MANCHES COOPER (Sep.03, 2023, 7:46 PM), https://www.penningtonslaw.com/news-publications/latest-news/2020/gdpr-in-sport-trying-wearables-on-for-size
[24] The Digital Personal Data protection Act, 2023, § 2(g), No. 22, Acts of Parliament, 2023 (India).
[25] The Digital Personal Data protection Act, 2023, § 18, No. 22, Acts of Parliament, 2023 (India).

The most dreaded threat in the realm of data security is undoubtedly a data breach or loss resulting from a breach. Such incidents can manifest in various forms, including external attacks, ransomware infections, computer or tablet loss or theft, or unauthorized access to peripheral systems leading to central archive breaches. With the implementation of the DPDP Act, brands with less robust security systems will find themselves exposed. Retailers are now legally obligated to promptly notify both their customers and the Data Protection Board in case of such breaches.[26] This requirement addresses past issues where some retailers lacked transparency, urgency, and, in some instances, honesty when handling data breaches. The new regulation compels retailers to adopt transparency in their approach to security breaches, thereby unveiling the vulnerabilities of certain websites. This, in turn, poses challenges to brand safety, trustworthiness, and credibility. Thus, the rights of data principals are the central part of the DPDP Act: the possibility of exercising rights not as simple consumers but with reference to the data concerning one's person.[27]

The act, without a doubt, offers a light of hope for counterbalancing the interests of data principals while acknowledging practical problems that enterprises may confront. It has piqued the interest of all parties, and it remains to be seen what shape it will finally take.[28] Furthermore, the Act must constantly adapt to new digital settings and emerging dangers because to the rapid rate of technology progress. One significant problem is achieving universal compliance across many industries, including the fashion industry, and organisational sizes. Balancing the requirement for data privacy with the facilitation of lawful data usage for innovation and research is likewise a difficult task.[29]

The exemptions granted by the government under the DPDP Act have raised concerns regarding their alignment with the doctrine of proportionality outlined in the Puttaswamy judgment[30]. Notably, consent is waived in specific situations, such as medical emergencies during epidemics and circumstances related to employment, including safeguarding employers

---

[26] The Digital Personal Data Protection Act, 2023, § 8(6), No. 22, Acts of Parliament, 2023 (India).
[27] Giovanni Ziccardi, *Wearable Technologies and Smart Clothes in the Fashion Business: Some Issues Concerning Cybersecurity and Data protection,* 9 LAWS 2, 5, (2018), https://www.mdpi.com/2075-471X/9/2/12#metrics
[28] DATA GUIDANCE REGULATORY RESEARCH SOFTWARE, https://www.dataguidance.com/opinion/india-comparing-digital-personal-data-protection-0 (last visited Sep. 3, 2023)
[29] Michael L. Rustad, How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices, 52 Suffolk U. L. REV. 227 (2019).
[30] *Supra* note 17.

from liabilities and ensuring confidentiality. Furthermore, a significant concern arises from the absence of a right to data erasure concerning government data usage, potentially allowing government authorities to retain data to their advantage. Additionally, unlike the GDPR, which incorporates the "right to be forgotten" inclusive of the right to erasure, the DPDP Act does not explicitly provide for such erasure rights absolutely, marking a notable distinction. These challenges emphasize the need for further scrutiny and refinement of the DPDP Act to align with evolving data privacy principles.

IV. Conclusion

Now is unquestionably the time for all stakeholders in the fashion industry to take a proactive approach, eliminate any unnecessary data collecting, embrace best practises, and prepare how to execute the DPDP Act's objectives.[31] Industries and Corporations are tasked with addressing security risks associated not only with the hardware and software of devices but also concerning the data they generate, the utilized networks, authorized personnel, and the protocols and policies governing information processing, storage, and distribution within an organization.[32] The demand for such strategies continues to escalate for several reasons. Often, legal and regulatory frameworks take approximately five years to adapt to technological advancements. This implies that current laws may not adequately cover the myriad new threats arising from emerging wearable technologies.[33] Developers of these wearables consistently push the boundaries, creating increasingly advanced devices, thereby widening the gap between evolving technology and the existing legal framework, as exemplified by the DPDP Act of 2023.

To conclude, the DPDP Act represents India's resolute commitment to safeguarding the personal data of its citizens in a digital age. While mirroring some principles of the European GDPR, it carves its path, uniquely tailored to India's diverse and dynamic landscape. Secondly, the challenges loom large. From concerns surrounding government exemptions to the evolving gap between technological advancements and regulatory adaptation, there is much ground to cover. Yet, amidst these challenges lies an unmistakable opportunity. The DPDP Act, with its stringent provisions and proactive stance, provides a robust foundation for responsible

[31] Lorna Cropper, Wearable Technology and the GDPR, SCL (Sep.03, 2023, 8:02 PM), https://www.scl.org/articles/3597-wearable-technology-and-the-gdpr#:~:text=In%20general%2C%20in%20order%20to,to%20use%20the%20wearable%20device.
[32] *Supra* note 10 at 621.
[33] *Supra* note 10 at 622.

innovation in the fashion-tech intersection. It underscores the need for businesses and individuals to embrace accountability, transparency, and education as they navigate this evolving landscape.