laws

Article

Wearable Technologies and Smart Clothes in the Fashion Business: Some Issues Concerning Cybersecurity and Data Protection

Giovanni Ziccardi [1]*

[1] Law Department «Cesare Beccaria», University of Milan, Milan, 20122, Italy ; giovanni.ziccardi@unimi.it
* Correspondence: giovanni.ziccardi@unimi.it; Tel.: +39-02-50312714 (F.L.)

Received: 21 April 2020; Accepted: 13 May 2020; Published: date

Abstract: Wearable devices and smart clothes give rise to pivotal technological and legal issues in the fashion business. The cybersecurity attention in the digital society, and the advent of General Data Protection Regulation No. 2016/679 (GDPR) in the European, and global, legal framework, implied the need to evaluate which norms and aspects of the European Regulation could apply to wearable devices, which are becoming more and more invasive. Wearable devices are, first of all (and from a data protection point of view), intrusive tools that can put users' personal (and intimate) data at risk. In particular, we will discuss the aspects of the spread of an accountability "culture" (also) in the fashion business, the need for correct management policy of data breaches, the rights of transparency for users/customers who are using wearable devices and smart clothes, and respect for the dignity and nondiscrimination of the individual during the data collection and processing. These are, all, fundamental points: the protection of the individual's data in the digital landscape is, in fact, strictly connected to the protection of his/her fundamental rights in the modern digital society.

Keywords: wearable devices; GDPR; data breach; smart fashion; smart clothes; transparency; privacy; data protection; legal informatics; cybersecurity

1. Introduction

Several recent field studies and business reports prospected, in the last two years, the fact that the wearable technologies market will have a strong impact and an unstoppable growth, even in the fashion sector (CCS Insight 2019). These studies described a wearables market worth $34 billion by 2020 and an existing solid presence of wearable technology in the digital society, with multiple applications in the retail, automobile, medical, and insurance sectors (Arnault 2018).

On the one hand, in fact, technologies are getting smaller. On the other hand, all the objects that surround us are designed to "contain" a specific technological device.

This market includes companies inventing, designing, and building miniature body-borne computational and sensory devices and creating wearable devices that can be worn under, over or in clothing, or, of course, "may also be themselves clothes" (Mann 2012).

In fashion shows, and in the most important events around the world, the first prototypes presented aroused wonder and admiration on one side, and concern on the other; also, the apparel industry is going "through a period of fast tech-driven transformations, with fashion brands working hard to capture the needs of the modern fashion consumer" (Arnault 2018).

In this case, as it is clear, digital fashion joins fashion in the strict sense, given that most digital objects have also become fashion or design garments.

The evolution consists in the fact that "wearable technology found in modern fashion garments are no longer just smart sensors but have evolved into being part of a complex ecosystem comprising sustainable and innovative apparel, aiming for a cleaner industry and a healthier lifestyle" (Arnault 2018): contemporary fashion tech garments "are made from biomaterials such as leather from fungi and pineapple, textiles from algae, 3D printed rubber from recycled plastics, and lab-grown leather, all recorded on the blockchain" (Arnault 2018).

For reasons of space, we will not deal with the interesting relationship between blockchain and data protection (there are many projects concerning the application of blockchain systems in the fashion sector), but there are several scholars who are tackling the problem in a very precise manner (Finck 2017).

From a technical point of view, therefore, these devices are interesting for the scholar for two reasons.

The first is that they are "real sensors": they contribute to building up the sensor society and are capable of capturing data from a person or his/her devices.

The second aspect is that these sensors communicate with the environment surrounding us, and being wearable clothes or objects, they communicate with all the other sensors they encounter during the movements of the same person who wears them.

The fashion world is trying, on one side, to radically change the wearable devices market: "This is a departure from the approach to date, where technical features have led the race, with most devices competing solely on battery life and capabilities. But technology is no stranger to fashion; from smart fabrics, models wearing Google Glass on the runway, to fashion designer Adam Selman sporting the next generation of payment enabled dresses on the catwalk–wearable tech is increasingly claiming its place in fashion" (Lambert 2019).

On the other side, legal scholars (Russey 2018) have started to try to connote with precision what is meant, from a legal point of view, as a "wearable device", "smart watches" (Chuah et al. 2016) or "smart clothes," the consequent legal implications, and what are the differences with respect to other technological objects and devices of daily use (like, for example, smartphones) (Kim 2016).

In our opinion, the difference between a smartphone and a wearable sensor is radical: the smartphone is invasive but remains disconnected from the human body and from the "physical" idea of "person." A sensor that enters the clothes, or is attached to a part of the user's body, becomes much more subtle (especially if the user, at a certain point, gets used to its presence and no longer realizes that he/she is constantly monitored).

On the one hand, therefore, the scholar notes an incessant evolution of the world of fashion that pursues, in many aspects, the evolution of technology and, above all, of technological society. On the other hand, the legal framework tries to adapt to the evolution of the digital society and, consequently, shows interest also for the fashion sector when countless devices of common use (sensors, Radio Frequency Identification systems, locators, touch screens, message or chat notification systems) enter clothes and the fashion business.

At the same time, these issues raise important cybersecurity problems, which need to be addressed in a summary way in order to better understand the consequent legal regulation as well.

This is why, in this chapter, we will have to deal simultaneously with business, technological, legal, and data protection issues. All four sensitively characterize the present and will probably characterize the future.

2. Data Processing and Cybersecurity in the Fashion Business

From a data processing, data protection, and cybersecurity point of view, two types of objects/devices in the fashion business can be identified, and they are very different from each other.

The first one is, in fact, an object that is worn as an accessory: a watch, a necklace, a bracelet, an earring. This "object" can have some technological characteristics, or networking and wireless connection capabilities, as well as the ability to process data and communicate them to the user or to "the outside" (for example: to the producer of the device, or to a shop).

The second type consists of real "smart clothes": wearable garments that have the ability to interact with the body and the health of the person and act autonomously in the analysis of the data of the subject who is wearing them; garments that can monitor sweating and skin pores, health status, heart rate, or can check if the subject is healthy and fit in a given moment. They also could adapt, for example, the color of the dress to the color of the skin (analyzing, for example, a face more or less tanned).

Often, this second type of device is also connected to "smart shops," "smart factories," or "smart companies," in order to create a union that allows not only, for example, the control of a music stream with a tap on the dress, or to warn about the presence of threat factors in the external atmosphere (for example: a dress that can "hear" the presence of radiations, or gas), but also to change the configuration of the device and the reaction of the technology depending on the surrounding urban, shopping, or domestic situation.

This second type of wearable technology is clearly more interesting also from a legal point of view, because it is potentially more invasive with reference to the rights and freedoms of the individual (Katyal 2014).

This is the reason why wearable technologies and smart clothes, in the last few years, were also under the lens of jurists (Ching and Mahinderjit 2016) and cybersecurity and data protection experts (Burbidge 2019; Allery 2019).

The idea that the diffusion of objects with certain advanced functions can be not only related to "simple" smart glasses, or bracelets for fitness, or watches/smartphones, but also to real sensors that analyze our body and tell us (or someone else) if we are, for example, hypertensive, dehydrated, or if we need to drink or eat, or that try to communicate with our brain waves, or (perhaps in the future) with microchips implanted under our skin, raises interesting legal issues.

3. Some Preliminary Legal Issues

First of all, we are talking about technologies that, compared to other smart objects, are extremely "personal" (Satyanarayanan 2001) and, above all, invasive of the most intimate part of the individual (Pearce 2016).

These are devices that are not designed to create a network, or to share information with other people, but that aim to adapt to a specific person, continually acquiring data on that subject and, above all, constantly operating for that purpose, not only during working hours, but also during the night and in extremely personal (or intimate) environments and contexts.

Wearable technologies and smart clothes are, in other words, "environmentally conscious": they are constantly monitoring and observing everything that happens in the surroundings, and then generate a large amount of data ("big data") that give rise to interesting GDPR issues (Wachter and Mittelstadt 2019), especially concerning data protection during big data analysis (Zarsky 2017).

There is an important, preliminary distinction (Mann 2012) between "wearable" devices and "portable" devices, like handheld and laptop computers: in fact, Mann says, "the goal of wearable computing is to position or contextualize the computer in such a way that the human and computer are inextricably intertwined" (Mann 2012).

"In this sense"–Mann writes–"wearable computing can be defined as an embodiment of, or an attempt to embody, Humanistic Intelligence. This definition also allows for the possibility of some or all of the technology to be implanted inside the body, thus broadening from 'wearable computing' to 'bearable computing' (i.e., body-borne computing)" (Mann 2012).

The idea of "Humanistic Intelligence" is very interesting if related to the interaction capability of wearable devices and smart clothes: as Mann correctly states, "One of the main features of Humanistic Intelligence is constancy of interaction, that the human and computer are inextricably intertwined. This arises from constancy of interaction between the human and computer, i.e. there is no need to turn the device on prior to engaging it (thus, serendipity). Another feature of Humanistic Intelligence is the ability to multitask. It is not necessary for a person to stop what they are doing to use a wearable computer because it is always running in the background, so as to augment or mediate the human's interactions. Wearable computers can be incorporated by the user to act like a prosthetic, thus forming a true extension of the user's mind and body" (Mann 2012).

Today, wearable devices in the fashion world exist, basically, in three types/forms.

The first type is made by clothes that can "activate functions," for example, for cyclists (that can start specific tasks by simply touching the clothes), often connected to smartphones or other communication devices.

The second type consists in technical clothes designed for athletes, monitoring, for example, blood pressure and heart rate values.

The third type combines clothes, body, and technology, for example, showing the messages or tweets received on the surface of the dress itself, or changing the colors of the clothes depending on the context, on the skin, or on the mood of the subject.

Even the wearable technologies sector, as, in general, the Internet of Things sector (the two sectors are strictly connected), has been overwhelmed by the advent of new ways of doing business through the collection and use of big data, especially with reference to the profiling of the most intimate aspects of the consumer.

Hence, there is the need to rethink, from a legal point of view, the delicate issue of protecting this information, the connected possibilities of discrimination related to misuse or abuse of this information (Rodotà 2015), the risk to the customer's reputation and, in general, the profiling and management of data of all those customers who use similar devices.

There are several fundamental points, from a Legal Informatics point of view, that are of particular relevance for the interpreter: they are all linked to the concepts of "data protection" and "cybersecurity."

The first point concerns the new methods of commercial use of consumers' data, modern e-commerce and marketing activities, the constant customer profiling activity (that, we will see, has an important impact for the GDPR), and the consequent consumer protection linked to the use of similar devices (Burbidge 2019).

This is an area of study that, on the one hand, is linked to the traditional business and marketing activities of companies and that, on the other hand, is increasingly conditioned by the presence of the companies on social networks and the need to innovate the ways of disseminating commercial information based on the collection, in fact, of big data coming from the daily life of customers.

To this end, wearable devices and smart clothes allow the achievement of two objectives.

The first is a control, also from a "geographical" point of view (GPS), of the consumer, even in his/her shopping activities and paths. This factor becomes very important from a marketing point of view: fashion is a sector where the relationship between in-store purchases and online purchases is very problematic to analyze in modern days, and the capacity to monitor consumer paths at any time and in any place takes on an enormous value.

The second objective is the ability to generate a profiling activity that is more precise than all those previously carried out; above all, because it can finally involve sensitive characteristics of the client. This is the reason why this issue inevitably has to deal with data protection legislation which, especially in Europe, has always tried to limit as much as possible these procedures, while respecting the need for data circulation and the need for business.

These first two protection requirements have been accompanied by the necessary attention to possible data breaches, i.e., the "escape" of data collected (with consequent reputation problems and fines coming from local Control Authorities) and the use of chatbot, automated systems that must be transparent to the customer for correctness (the user must always be aware that he/she dialogues with a robot and not with a human being).

To these first problems, there are specific implications involving smart fabrics, nanotechnologies, and, generally, the Internet of Things. Wearable and connected technologies can be very useful, but they have security problems, as does the Internet of things in general: every device that is connected is vulnerable.

The implementation of the GDPR since May 2018 in all EU Member States has entered such a delicate and unstable framework and had to face new problems that are not easy to solve.

The idea of the protection of digital data is transversal to all the problems listed above.

4. Four Points of Discussion

It seems to us that there are four clear points of discussion that today concern wearable devices and smart clothes from a legal and data protection point of view:

(i) the need to introduce a new "culture" of data protection (training, for example, all the people who are processing data) when dealing with such intimate devices and data, especially if what is being processed is not only customers' data, but also information related to employees/workers (Allery 2019);

(ii) the need to plan correct data breach management, as the collection of large amounts of data made by these wearable devices and smart clothes will inevitably, sooner or later, lead to the threat of a data breach;

(iii) the need to guarantee a transparent legal framework regarding the delivery of the information, the collection of consent of the customer, and the development of less intrusive forms of marketing and targeting;

(iv) finally, the need to always guarantee the exercise of the rights of those who wear these devices, up to the cancellation of all customers' data and the disconnection of the device.

In this study, the four aspects indicated above will be in summary highlighted. We will try to link, in particular, the phenomenon of wearable devices and smart clothes to the GDPR norms, and to the most common cybersecurity approaches (and best practices).

5. Discussion

I. Wearable technologies and data protection norms

The General Data Protection Regulation (GDPR) is having a very strong impact on the world of fashion and on its commercial practices (Allday 2018).

The theme of data protection has become central and involves, today, both personal and particular (or "sensitive") data: types of data that, in the fashion world, are very common.

Data is instrumental in marketing, as Allday correctly states: "allowing retailers to bridge the gap between online/offline and digital/physical stores (where applicable), so retailers may struggle to maintain this without as much consumer information. Currently, the online shopping experience is often a 24/7 engagement, with emails landing throughout the night offering similar items to your shopping/browsing history. Without this constant presence, online fashion retailers will have to find less intrusive ways of keeping high levels of engagement with their consumers. Although companies will still be able to see what their customers are purchasing, there will be less scope for them to track closely their browsing habits and histories. The consumer's 'right to be forgotten' must be addressed within one month, and customers will also have the right to have their personal data erased. Although thousands of fashion products sold online are inspired by luxury catwalk items, trends are equally driven by consumer shopping habits and patterns. If customers request that they be erased from retailers' systems, it could limit insights into what their customers are looking for next" (Allday 2018).

As Allday says: "online fashion companies will have to change the way they interact with their customers and use their personal information. For pure play retailers like Amazon, ASOS, Boohoo and Missguided, all of whom have benefited from the ambiguity of the EU's existing data laws, the General Data Protection Regulation has the potential to drastically, perhaps catastrophically, alter how they operate" (Allday 2018).

Also the presence on social media of the most important brands in the fashion industry will change: "Lax data laws have allowed fashion retailers to leverage social media even more by offering personalised shopping links that lead to clicks and therefore sales. Online fashion brands are faced with the momentous task of overhauling not just their business strategy, but ensuring that their brand identity is not watered down by GDPR" (Allday 2018).

First of all, as Arthur correctly writes (Arthur 2016), from a data processing point of view, some of these wearable devices and smart clothes "even stretch what the term 'wearables' might mean–stepping beyond connected textiles into deeper fibre science, which is the area looking the most likely to shape the future of our wardrobes" (Arthur 2016).

The author cites, for example and among others: Levi's and Google Project Jacquard ("a piece of wearable technology designed for urban cyclists. Conductive yarn is weaved into the left cuff enabling touch interactivity so users can tap, swipe or hold to fulfill simple tasks like changing music tracks, blocking or answering calls or accessing navigation information delivered by voice"); The Unseen for Selfridges ("a start-up that has captured the simple idea of colors that alter based on user interaction or the environment they're placed in. The resulting line of luxury accessories for Selfridges […] included a backpack, scarf, phone case and more, which responded to things like air pressure, body temperature, touch, wind and sunlight. An Italian alligator-skin shoulder bag for instance saw environmentally-responsive ink shifting from black in the winter, to red in the spring, blue in the summer and green fading to red in the autumn"); and Emel+Aris (a smart coat with hidden intelligent heating technology inside: "Made from a lightweight polymer, rather than a load of wires, it produces FIR (far infrared) heat energy from various panels across the garment that is then absorbed by the skin to heat the muscles and increase blood flow") (Arthur 2016).

In 2017, in another example, University of Manchester's National Graphene Institute "produced a dress in collaboration with wearable tech company Cute Circuit. The dress is made with a fabric that has 'wonder material' graphene which causes the dress to change color according to the wearer's breathing patterns" (Draper 2018).

We are therefore in the presence of technologies that are not just wearable objects, but are real tools for the transmission of data and are particularly complex technologies in their functions (even invasive of the privacy of the individuals). In other words, we are in the presence of potentially dangerous technologies for human beings.

So, the first necessary point, when discussing the (cyber) security of wearable devices and smart clothes, is to understand the need for the diffusion of a "culture" of data protection that, in many cases and due to security costs, has not been implemented.

This must be done even before designing such tools, and must become an essential part of the production process itself of these products.

In a period of market crisis, investments in information security have been minimal: often these are the first balance voices to be cut. However, at the same time, there is a commercial rush to collect data. This commercial rush is arising new legal challenges (Mathys 2014).

The GDPR, first of all, demands, with a particular attention to the idea of accountability, that the security must be placed "inside" the device itself, and the accountability must be "inside" the company itself. Also, this approach must be demonstrable at any time.

This entails the need for large-scale training of all operators, from the top to the subjects who process the data, to ensure a safe and secure data environment. This can happen with ad hoc training and with the writing of policies, regulations, and best practices.

This first, general point is clearly described in the text of Article 32 of the GDPR: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."

The big news of the GDPR is that it leaves the company free to decide how to implement security measures in its specific reality. There are no longer any lists of mandatory measures, but it is up to the data controller to decide which measures to implement. This is a completely new approach that will be tested in the coming years.

The description of the risks strictly connected to data processing are in the second paragraph of Article 32: "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed."

This means that anyone who produces wearable devices and smart clothes, or whoever resells them, must, before starting to make use of these tools and give them to their customers, evaluate the possible risks and prepare safety measures that protect the processed data.

Concerning, finally, the diffusion of a "culture" of data protection, paragraph 4 of Article 32 of the GDPR is clear: "The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he/she is required to do so by Union or Member State law."

This is a central aspect: all data processors must first be trained on data protection issues. This becomes particularly important when smart devices communicate, for example, with a store and not directly with the factory. All the subjects who process the data, even those with less important or temporary job positions, must be aware of the existence of the legislation on data protection and on the best ways of protecting customer data.

The second crucial point, the data breach management, involves the most important threat connected to the collection of data using wearable devices today. Understanding how to recognize a data breach, how to manage it (to avoid millionaire fines), how to report it to the supervisory authority but also to customers, and how to manage the data breaches that may not take place on site but in shops, stores, or companies connected to the main factory is linked to the ability to know how to assess risks of image, reputation, discrimination, possible identity theft, and economic losses.

The norms related to data breach are included in Articles 33 and 34 of the GDPR. Article 33 states that "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 h after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 h, it shall be accompanied by reasons for the delay."

Article 34 indicates that "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay." However, "The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach; in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."

Then, there is the fundamental aspect of transparency, along with information and collection of consent, which have always been central to the European data protection system. This directly involves targeted marketing and profiling but also spam, newsletters, apps, and websites.

Finally, there is the aspect of the exercise of rights, especially with the request to delete and update the databases.

At the center of all these four aspects, there is the general idea of accountability, i.e., the entire system must be framed around the idea of protecting the data by design and by default, and all this must be demonstrable.

Privacy and security, in conclusion, are at the heart of wearable technologies, and they are two different aspects. The main risk is obviously the direct collection of sensitive data that these devices make, such as precise geolocalization, credit card numbers for possible payments, information on health status, and collection of habits and physical condition for a long period of time.

II. The specific accountability issues of wearable devices and smart clothes

The starting point, even in the context of wearable devices and smart clothes, is the understanding of 'accountability,' the new security approach required by the GDPR to set up corporate and productive activities and personal data handling from a correct data protection perspective.

The idea of accountability consists in doing and demonstrating (in other words, in "creating"), an environment aimed at data protection, and being able to document and prove it anytime.

The first step is usually considered that of training: training all operators so that their behavior is correct and aimed at protecting the data while not hindering its circulation. Particular attention, also in the fashion world, should be paid to three areas: (i) marketing and sales, (ii) human resources, and (iii) information technology staff. These are the three most vulnerable sectors.

Marketing and sales will have to pay particular attention to information, especially for TV spot, web, and app activities and highly targeted campaigns, including campaigns based on the physical characteristics of customers and the management of large databases. Human resources will have to pay particular attention to the protection of employee data, especially if wearable devices are given also to the staff. The IT department controls the whole data system and the processing and protection of the information.

In practice, in all these three areas, accountability is achieved through a list of fulfillments: the information and consent, the appointment of a Data Protection Officer, the keeping of a treatment register, the assessment of the risk and impact in the case of particular treatments, the contractualization of relations with external processors, and a framework of security measures also made up of training and policy plans for managing data breaches, phishing attacks, and payment systems fraud.

Companies should ensure that all of their employees' practices are aimed at promoting data security and, above all, human resources staff must establish policies, business operations, and contracts with employees that take into consideration the use of wearable technologies in the workplace. The essential problem, in this case, is the privacy of the worker, especially the violation of privacy and the risk of spreading sensitive information about the worker. They must be able to choose whether or not to wear the device, and the functioning must be transparent and well illustrated. Furthermore, the devices must not function beyond working hours.

III. Wearable Technologies and Data Breach Issues

The data breach, or data loss following a violation, is the most feared threat. It can happen in many ways: an external attack, but also a ransomware virus, loss or theft of a computer or tablet, access to a peripheral system that allows access to the central archive. In this case, transparency towards the supervisory authority and the users has become essential, especially if customers' rights are at risk.

The management of a data breach therefore entails an initial assessment of the risk, to frame the event in a simple accident, where an incident log will be held, or in a serious event that must be reported. The first comparison will be with the supervisory authority, and must be reported within 72 hours in specific ways. The second comparison will have to be with users in order to inform them, and here the reputation problem of the company is the most important issue. The preparation of a policy with both internal purposes (keeping track of all incidents) and external purposes (specific methods for managing and communicating data breaches) is essential.

Given the great risks, companies that develop wearable technologies should implement appropriate cybersecurity measures. There is no standard checklist, but measures must be adapted to the situation (for example: the volume and nature of the data collected, and the cost of a potential data breach as an impact on people's rights). Certainly, the protection should already be incorporated when thinking about the product and developing it ("privacy by design"), and the subject should have full control of his/her device.

As Allday correctly notes, GDPR will also "expose brands whose security systems are not as sophisticated as they should be, as retailers will be required to notified regulators of any data breach within 72 h and in some case, they will be legally obliged to notify their customers too. Before, some retailers lacked transparency, urgency and in some case, honesty, when dealing with data breaches. Forcing retailers to be transparent when it comes to security breaches will expose certain websites' shortcomings, which challenges brand safety, reliability and credibility" (Allday 2018).

Another key point will involve exactly how retailers remove their consumers' data, particularly when information is stored on several distinct databases: "For some companies, a complete redesign of internal IT systems will be required; for others, it will be a matter of whether a customer's data is anonymized or completely deleted, and whether it will be possible to mix the two actions within one database" (Allday 2018).

The new regulations also "make clear that it is not just the IT departments of retailers who should be clued up on data breaches and their prevention, but all members of the corporation, no matter what level, as well as third party affiliate companies, such as PRs, freelancers, insurance companies and recruiters" (Allday 2018).

IV. Transparency and consumers attention

In the GDPR system, the principle of transparency is closely connected to the idea of information and consent. The disclosure/information notice is an essential requirement that allows you to inform the user about how the data will be processed. The contacts, purposes, legal basis, data retention period, and transfer (or not) abroad are the most important points, to which are added the recipients and the possibility of exercising their rights.

Consent is now given in electronic format and poses the problem both of verifying the age and the will of the subject, and of filing it to verify possible revocations.

Most of the data concern health and fitness, the steps taken every day, sleep cycle, calories burned, and these are all data that, if exposed, would make the subject very vulnerable.

The large volume of so much data allows analysis to be carried out by those who have access to this data, which would not be possible with smaller datasets. Furthermore, data relating to habits could be used for other purposes, such as insurance purposes, or employee control. Transparency, with such types of data, means knowing who the data owner is, where data are stored, if they are encrypted, how they can be used and if they can be resold.

It is therefore essential to draft terms of services and privacy policies that highlight which data are collected, how they are stored, their use, if third parties are involved in management, and security measures. The collection and storage of data should then be limited, and the encryption of information should be the standard.

Attention to the consumer must also be connected to the profiles of responsibility connected to the product and to its functioning. The brand is exposed to possible responsibilities, both for physical damage and for the possibility of distraction by the user while driving or walking, or for damage to third parties.

The rights of data subjects are the central part of the European system: the possibility of exercising rights not as simple consumers but with reference to the data concerning one's person. The right to be forgotten, but also the rights to rectification, or the acquisition to treatment, are central.

As Allday states, online retailers "must therefore find ways of leveraging their loyalty schemes and other forms of advertising without creating a retail space in which legal consent is required from the consumer. The success of data-driven advertising has been, in part, down to the fact that so many consumers are unaware of it. When presented with a box on the screen asking if you want to give away your personal details, many people would say no. 'Consent' is often built into the cookies that the average Internet user accepts without reading the T&Cs. The new limitations will require more traditional, less intrusive forms of targeted advertising, which will involve looking to more authentic advertising used in physical stores. Euromonitor figures show that online fashion retailing now accounts for 20% of all apparel and footwear sales in the UK and 15% in the whole of Western Europe, but GDPR will drastically alter the landscape of fast fashion if the key players do not address and adapt to the new, more private shopping landscape online" (Allday 2018).

In our opinion, even if the issues of transparency and consensus are not strictly related to the technological aspect of the topic we are dealing with (i.e., the hardware that collects the data), they are still central in view of a broad spectrum of protection. Even the fashion industry has long based its activity on data processing, and correct information, related to a clear manifestation of will, assumes central importance in the more general framework of data protection.

6. Conclusions

The fashion sector will most likely be affected by the new regulatory framework brought by the GDPR; the same will happen for wearable devices and smart clothes, which will probably play an increasingly important role in the near future.

Some data protection issues are common to all commercial sectors and all digital technologies, from network connectivity to the use of smartphones; others are more specific, and peculiar, to wearable devices. In particular, the management of big data of customers and workers (Allery 2019) collected in these ways will be a central problem in the near future, along with profiling and marketing activities aimed at collecting and processing such data. This aspect, however, is common to many commercial sectors and does not present particularly innovative features in the topic we are dealing with.

In our opinion, a peculiar feature that will concern the relationship between fashion and data protection will be the close connection between the data and the human person (and its everyday life). For the first time, the same clothes that the subject will wear will also function as sensors to collect, in real time, a large amount of data. This will cause such actions to be perceived as invasive, able to penetrate into the depths of the person and, therefore, more urgent to regulate from a legal point of view.

The vulnerability of the data must be taken into consideration, not only for the value that the commercial archives have, but because we are discussing data, in this case, which must be considered critical and sensitive, given their close connection with the person. The creation of an ad hoc policy on security and privacy, which is usually more common in other areas (i.e., banking, insurance, telecommunications, public sector), is today essential also in the fashion sector.

We refer, in particular, to a policy that is able to better prepare all the subjects who process the data to deal effectively with a data breach. The essential points of such a policy, for example, could be the following:

1. Understand what a data breach is and be able to identify it and communicate it to security personnel. Remember that a data breach, from the point of view of the GDPR, is not only an attack on data from outside, but also a defect or vulnerability of an app or electronic bracelet or a smart device that can cause uncontrolled spreading of data.
2. React with particular urgency as soon as you know the data breach and also provide some basic essential information to understand the seriousness of the event.
3. Activate a communication flow both to the Control Authority and to the customers that allows the maximum transparency of the accident.
4. Immediately try to limit the damage and its consequences.

There are two methods of protection that are most evident and that can be used to mitigate damages related to a data breach: (i) the use of anonymous data, and (ii) the encryption of information.

If we extrapolate anonymously a profile of each user of a brand, which contains interests based on the places the customers frequent, it can allow for detecting interesting data and implementing different strategies depending on the level of brand affinity and also on physical movements, even if the data is processed anonymously.

It becomes useful, in fact, to know how to dominate and govern data throughout the customer journey, made of many stages in the offline and online world, focusing on "location intelligence" to analyze in-store traffic, to understand the tastes of customers around the world, and to present personalized and hyperlocalized offers.

Then, there will be an almost exclusive importance of mobile technologies, since the data collected through the mobile devices of the customers will be integrated with artificial intelligence technologies (Luce 2019) able to predict consumer behavior and offer advice through virtual assistants.

This point is, from a legal perspective, very interesting. Several scholars are studying the existence of a 'right to explanation' (Edwards and Veale 2017) of all decisions made by automated or artificially intelligent algorithmic systems as a tool to enhance the accountability and transparency of automated decision-making (Wachter et al. 2017).

All the fashion houses are, these days, equipping themselves with data scientists who know how to analyze this enormous amount of data and generate new value. Less attention is devoted to the recruitment of legal and cybersecurity experts.

The hard point is that real anonymization is becoming increasingly difficult due to the constant possibility of correlating data and information.

The wearable technologies are the most suitable for perfecting this data collection, as they follow the movements of the individual and collect data closely related to the personality (and also to the health) in all moments of the individual's life, both private and in society. It is an enhancement of the advertising possibilities that has no equal, especially if combined with artificial intelligence, machine learning, and virtual and augmented reality (Kamarinou et al. 2016).

So, the first point of conclusion is that processing data as anonymously as possible becomes essential.

The second aspect, data encryption, in addition to anonymization, seems to be the most effective technical tool for protecting data after the collection and, above all, when the individual communicates, through the wearable devices, with the fashion company.

The norms and, in this case, the GDPR clearly recall these needs to protect the customer who wears the device: an anonymous processing of the data based on security and encryption.

To this end, the wearable devices that will be created, or have already been created, with privacy and security in their DNA will certainly succeed in combining efficiency and new marketing opportunities with the protection of people's rights.

Allday, in conclusion, highlights four interesting focal points that we can use to connect the wearable devices world, the cybersecurity best practices, and the GDPR:

(i). It is essential to guarantee, first of all, that all "staff members are made aware of what constitutes a data breach; how serious they are, no matter how few people may seem affected initially; how to report them; how to prevent them" (Allday 2018). The data breach, it was said, is seen as the first and the most important threat, with reference to data collected through wearable devices and smart clothes. It is the idea that the most intimate data of people, closely related to the body, can come out and be made public, or violated.

(ii). Then, it is important to invest in "Customer Relationship Management, both to allow customers a human point of contact for questions and queries regarding their personal data, and to maintain personal engagement between the retailer and consumer that could suffer as a result of GDPR" (Allday 2018). This second point concerns respect for the consumer also from a data protection point of view, which is reflected in the many actions and obligations provided by the GDPR.

(iii). More, it is fundamental to be "transparent with customers about exactly what their rights are, how they can request more information and how they can have their data removed. As the world saw in the wake of the Cambridge Analytica and Facebook scandal, transparency and honesty are both vital to keep customers loyal and to ensure that they feel safe on the Internet" (Allday 2018). From this point of view, it becomes important to respond immediately to any request from customers concerning their data (we find that the requests for cancellation of the information are, in this perspective, the most important).

(iv). Last, but not least, it will be important the focus on "social media marketing and advertising to ensure personalized content that keeps individual consumers engaged and interested in the brand, without their data being compromised or exploited" (Allday 2018). It will be important, in particular, to find a good compromise between the data protection needs and the need, in the digital society, to process data with great speed and precision.

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflict of interest.

References

(Allday 2018) Allday, Florence 2018. *Is the Fashion Industry ready for GDPR?* London: Euromonitor International. Available online: https://blog.euromonitor.com/fashion-industry-ready-gdpr/ (accessed on 25 May 2018).

(Allery 2019) Allery, Charlotte 2019. Wearable Technology in the Workplace and Data Protection Law, retrieved from ComputerWeekly.com, February. Available online: https://www.computerweekly.com/opinion/Wearable-technology-in-the-workplace-and-data-protection-law (accessed on 26 February 2019).

(Arnault 2018) Arnault, Laurenti 2018. The Only Thing That Buyers Want from Wearable Technology Fashion, WTVOX, 30 July. Available online: https://wtvox.com/fashion/wearable-technology-fashion/ (accessed on 30 July 2018).

(Arthur 2016) Arthur Rachel 2016. The Future of Fashion: 10 Wearable Tech Brands You Need To Know, Forbes, 30 June, Available online: https://www.forbes.com/sites/rachelarthur/2016/06/30/the-future-of-fashion-10-wearable-tech-brands-you-need-to-know/#5faad8b14220 (accessed on 30 June 2016).

(Burbidge 2019) Burbidge, Rosie 2019. *European Fashion Law*. Cheltenham: Edward Elgar.

(CCS 2019) CCS Insight Study: Wearables Market to Be Worth $25 Billion by 2019. Available online: https://www.ccsinsight.com/press/company-news/2332-wearables-market-to-be-worth-25-billion-by-2019-reveals-ccs-insight/ (accessed on 29 October 2015).

(Ching and Mahinderjit 2016) Ching, K., and S.M. Mahinderjit. Wearable Technology Devices Security and Privacy Vulnerability Analysis. *International Journal of Network Security & Its Applications* 8: 19–30. doi:10.5121/ijnsa.2016.8302.

(Chuah et al. 2016) Chuah, Stephanie Hui-Wen, Rauschnabel, Philipp, Krey, Nina, Nguyen, Bang, Ramayah, Thurasamy and Lade, Shwetak. 2016. Wearable technologies. The role of usefulness and visibility in smartwatch adoption. *Computers Human Behavior* 65: 276–84.

(Draper 2018) Draper, Sam 2018. *Are Smart Fabric the Future of Fashion?* WT (Wearable Technologies): 82211 Herrsching am Ammersee, Germany Available online: https://www.wearable-technologies.com/2018/06/are-smart-fabrics-the-future-of-fashion/ (accessed on 12. June 2018).

(Edwards and Veale 2017) Edwards, Lilian, and Veale, Michael 2017. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for. *Duke Law & Technology Review* 16: 18. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855 (accessed on 24 May 2017).

(Finck 2017). Finck, Michèle 2017. Blockchains and Data Protection in the European Union. Max Planck Institute for Innovation & Competition Research Paper No. 18-01. *European Data Protection Law Review*, **2008**, *volume 4, Issue 1,* Pp 17–35. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322 (accessed on 6 December 2017).

(Kamarinou et al. 2016). Kamarinou, Dimitra, Millard, Christopher and Singh, Jatinder. 2016. *Machine Learning with Personal Data*, Queen Mary School of Law Legal Studies Research Paper No. 247/2016. Amsterdam: Elsevier. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811 (accessed on 8 November 2016).

(Katyal 2014) Katyal, Neal. 2014. Disruptive Technologies and the Law. *Geo. LJ* 102:1685–89.

(Kim 2016) Kim, Young Ah. 2016. New Legal Problems Created by Wearable Devices. *Illinois Business Law Journal* Available online: https://publish.illinois.edu/illinoisblj/2016/02/29/new-legal-problems-created-by-wearable-devices/ (accessed on 29 February 2019).

(Lambert 2019) Lambert, Jorn *Technology and Fashion Unite as the Wearable Market Matures*. TechRadar: New York, NY 10036, US. Available online: https://www.techradar.com/news/technology-and-fashion-unite-as-the-wearable-market-matures (accessed on 22 February 2019).

(Luce 2019) Luce, Leanne. 2019. *Artificial Intelligence for Fashion: How AI is Revolutionizing the Fashion Industry*. San Francisco: Apress.

(Mann 2012) Mann, Steve 2012. Wearable Computing. In *The Encyclopedia of Human-Computer Interaction*, 2nd ed. Edited by Mads Soegaard and Rikke Friis Dam. Idea Group Reference: Hershey, PA 17033, US. Available online: http://www.interactiondesign.org/ encyclopedia/wearable_computing.html (accessed on 31 December 2005).

(Mathys 2014) Mathys, Roland 2014. Legal Challenges of Wearable Computing, 30 April. Available online: https://www.swlegal.ch/files/media/filer_public/2c/7a/2c7a67fa-96ed-489e-981f-6c10d0266326/140801_roland-mathys_legal-challenges-of-wearable-computing.pdf (accessed on 30 April 2014).

(Pearce 2016) Pearce, Sarah 2016. Wearable tech and data privacy: What you need to know. *UKTN*, October 25. Available online: https://www.uktech.news/news/wearable-tech-privacy-issue-20161025 (accessed on 25 October 2016).

(Rodotà 2015) Rodotà, Stefano 2015. *Il Diritto di Avere Diritti*. Roma and Bari: Laterza.

(Russey 2018) Russey, Cathy 2018. *How to Limit Legal Risks that Come with Wearable Devices*. City: 82211 Herrsching am Ammersee, Germany. WT (Wereable Technologies). Available online: https://www.wearable-technologies.com/2018/11/how-to-limit-legal-risks-that-come-with-wearable-devices/ (accessed on 13 November 2018).

(Satyanarayanan 2001) Satyanarayanan, Mahadev 2001. *Pervasive Computing: Vision and Challenges*. IEEE Personal Communications. Available online: http://www.cs.cmu.edu/~./aura/docdir/pcs01.pdf (accessed on 31 August 2001).

(Wachter and Mittelstadt 2019) Wachter, S., and B. Mittelstadt. 2019. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review* 2019: 494. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829 (accessed on 5 October 2018).

(Wachter et al. 2017) Wachter, Sandra, Mittelstadt, Brent and Floridi, Luciano. 2017. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law* 7: 76–99. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 (accessed on 24 January 2017).

(Zarsky 2017) Zarsky, Tal. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review* 47: 995. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646 (accessed on 22 August 2017).