Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations*

Manuel David Masseno
Cristiana Santos

Abstract

Data lies at the core of all smart tourism activities as tourists engage in different and personalized touristic services whilst the pre/during/post travelling or in holidays. From these interactions, a digital data trail is seamlessly captured in a technology embedded environment, and then mined and harnessed in the context of STD - Smart Tourist Destinations to create enriched, high-value experiences, namely those related to eco-responsibility, as well as granting destinations with competitive advantages. The perceived enjoyment of experiences must be considered within the legal framework of Privacy and Data Protection by exposing inherent risks, analysing the available answers given by the GDPR – the General Data Protection Regulation of the European Union. Hence the purpose of this paper is i. to singularize the specificities of Smart Tourism Destinations; ii. to show how the principles of personal data protection, as set forth by the GDPR, are allocated within the STD realm; iii. and, finally, to derive potential legal implications of this ecosystem. Our approach is based on a legal analysis engaged in scholarship research. We have mostly denoted the underestimation of the legal implications of technology-enhanced tourism experiences, and the marginalization of both informed involvement and awareness by the individual in these processes. This study is novel in having undertaken an initial exploration of the legal implications of experiences taking place by STD.

Summary

Keywords: Privacy, Data Protection, Smart Tourism Destinations, GDPR, Touristic Services

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

1. Introduction

Smart Tourism Destinations (hereinafter called STD) are an offspring of the technological foundations of Smart Cities, themselves benefiting from the interplay with other technological environments based on the Internet of Things (IoT) and the Cloud, as enabled by Big Data Analytics.

However, while these subjects have been examined extensively within Privacy literature, their specific context and legal consequences on STD is still to be explored. As a matter of fact, this is perceived and pointed out as a missing issue by the Tourism Science literature regarding STD[1]. Given the insufficiencies in the literature and these recent claims, this study aims to provide a theoretical review of the technology-empowered tourism experiences and its legal implications to privacy and data protection. Theoretically and in practice, STD have been designed to enrich tourism experiences and to enhance the competitiveness of each destination.

ICTs embedded within tourism destinations environments allow the collecting and analysis of large amounts of tourism data for the identification of attitude patterns and to predict behaviors of tourists and travelers. This is achieved by addressing their potential needs and desires even at an unconscious level of travelers.

Regarding this connection between Tourism and ICTs, we're facing a new relationship between clients-tourism providers which is very context-specific: i.) Short-lived engagement, focused on the pre/during/post travel, which makes trust-building and costumer's loyalty much harder[2]; ii.) Imminent need for real-time information *in situ,* for vacation decision-making, so that tourists might be easily persuaded to forego their data; iii.) Heightened benefits or "perceived enjoyment" (evoked by the engaging content, discounts, and interactive system features)[3], suggesting that personal data is traded therewithal for useful purposes and hence privacy concerns might be temporarily suspended; iv. Tourism activities take place in locations outside of the usual realm of the traveler, and are often facilitated by unknown local service providers, which decrease privacy risk perceptions[4], for instance at natural spaces apparently far from urban invasive surveillance; v. Growing number of connected smart objects and wearable devices involved in a network of multiple vendors and interoperating systems, where privacy issues are blanked out; vi. Multiple stakeholders' interaction making it even harder to identify privacy flaws.

The following illustrative examples provide insight towards the personalized and smart added-value services that STD can offer:

[1] Even being tourism the world's largest industry, with receipts of almost 1,200 USD Billion in 2017, and growth expectations of 4% to 5% for 2018, according to the UNWTO Barometer, notwithstanding internal tourism.

[2] B. Neuhofer – D. Buhalis et al., *Smart technologies for personalized experiences: a case study in the hospitality domain*, in *Electronic Markets*, vol 25, issue 3, 2015, 243 ss.

[3] *Ibidem.*

[4] U. Gretzel, Ulrike – M. Sigala et al., *Smart tourism: foundations and developments*, in *Electronic Markets*,vol. 25, issue 3,179 ss.

Full historic immersions through smart optics devices or augmented reality for a "happy guest" are services already offered. Further, location-based services (LBS) could alert users to the closeness of birds to be watched or to endemic plants. Besides, estimated waiting time for the entrance to Natural Parks and other Protected Sites can be accurately quoted, to the minute, so tourists may reorganize their visiting or trail options or get a drink in a bar while waiting. Besides, aware on customers' special dietary circumstances in regard with their medical condition, as well as religion restrictions, tourism service providers may provide for meals that suits their preferences. As for transport, real-time information about the tourist's destinations, which direction to get on, and the ability to respond (i.e., by suggesting alternatives) to unpredictable events in real-time are envisioned, namely sudden weather changes. RFID tags on their outfit would make it easier to locate travelers in case of being lost or in order to identify those liable for damages inflicted to natural spaces or protected species.

All these enhanced services allow tourists to get much more from their travel and helps them fulfilling the experiential travelling potential of the destination[5]. STD experiences are hence achieved through intensive personalization, context-awareness and real-time monitoring[6]-[7] processes of information management which entail legal risks, demanding a careful analysis within the data protection framework.

Given the nature of STD and its uses, the application of some of the principles of data processing (*e.g.* the principles of data minimization, purpose limitation, fairness and transparency, and free, specific and informed consent) may be challenging in this technological scenario.

As a large spectrum of user-generated content is tourism data processed in a smart tourism environment concern personal data and human interaction, there is a direct impact on individuals and their rights with regard to the processing of personal data.

As explicitly mirrored in Article 8 (3) of the Global Code of Ethics for Tourism[8], tourists and visitors should benefit from the same rights as the citizens of the country visited concerning the confidentiality of the personal data and information concerning them, especially when these are stored electronically. Therefore, it should be underlined that Privacy and Data Protection evaluation is needed in any tourism environment, balancing the tradeoff value and affordances added by STD and its legal protection. This work therefore provides a study of the principles of data protection, as set forth by the GDPR, within the STD context.

The paper is organized as follows. Section 1 explains the background of STD, describing briefly its specificities and giving examples of technologically enhanced and

[5] D. Buhalis – A. Amaranganna, *Smart Tourism Destinations*, in Z. Xiang – L. Tussyadiah (eds.), *Information and Communication Technologies in Tourism 2014 - Proceedings of the International Conference in Dublin, Ireland*, Heidelberg, 2014, 553 ss.

[6] *Ibidem.*

[7] D. Buhalis - A. Amaranganna, *STD: Enhancing Tourism Experience Through Personalisation of Services*, in L. Tussyadiah – A. Inversini (eds.), *Information and Communication Technologies in Tourism 2015 - Proceedings of the International Conference in Lugano, Switzerland*, Heidelberg, 2015, 377 ss.

[8] Accessible online at www.ethics.unwto.org/.

empowered experiences. Section 2 explains how smart technologies affect compliance with the principles of the General Data Protection Regulation[9], as the current basis of Privacy and Data Protection Legal system in the European Union. Section 3 concludes the paper and provides some clues for future directions.

2. Specificities of STD

This section describes the constituents of STD, objectives and derived added value.

2.1. Smart Tourism Destinations

In order to characterize more closely the utility functions layered in tourism destinations, it is worthy to point out that successful destinations are composed by five tourism dimensions: transportation, accommodation, gastronomy, attractions and ancillaries services, which can be then structured into six axes or "6As" as the literature describes[10], namely: i. Attractions, which can be natural, like as mountain or a seaside; artificial, as amusement parks or sports facilities; or cultural such as music festival or a museum; ii. Accessibility refers to the transportation within the given destination; iii. Amenities characterize all services, namely accommodation, gastronomy and leisure activities; iv. Available Packages; v. Activities; and vi. Ancillary Services (e.g. daily use services such as bank, postal service and hospital).
By applying *smartness* into tourism destinations, STD are defined as:
«[…] tourism supported by integrated efforts at a destination, to find innovative ways to collect and aggregate/harness data derived from physical infrastructure, social connections, government/organizational sources and human bodies/minds in combination with the use of advanced technologies to transform that data into enhanced experiences and business value-propositions with a clear focus on efficiency, sustainability and enriched experiences during the trip»[11].
This embracing concept comprises three core elements of destinations[12]:
i.) Reliance on smart technology infrastructures, wireless sensor networks (IoT) and integrated communications systems, e.g. sensor technology, ubiquitous wifi, near-field communication (NFC), smart mobile connectivity, radio-frequency-identification (RFID), sophisticated data warehouses; data mining algorithms, also considered vital to creating a smart technology infrastructure[13]. IoT provides support in terms of

[9] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), applicable from the 25th May 2018.

[10] D. Buhalis, *Marketing the Competitive Destination of the Future*, in *Tourism Management*, vol. 21, 2000, 97 ss.

[11] U. Gretzel – S. Reino et al., *Smart Tourism Challenges*, in *Journal of Tourism*, vol. 16, issue 1, 2015, 41 ss.

[12] M. Höjer – J. Wangel, *Smart Sustainable Cities: Definition and Challenges*, in L. Hilty - B. Aebischer (eds.), *ICT Innovations for Sustainability, Advances in Intelligent Systems and Computing*, Heidelberg, 2015, 333 ss.

[13] U. Gretzel – S. Reino et al., *op. cit.*

information gathering and analysis as well as regarding automation and control. For instance, chips embedded to entrance tickets, or a smartphone app, allow tourism service providers to track tourists' locations and their consumption behavior, enabling location-based advertising or rescue in case of them getting lost when departing from an usual trail. In addition, cloud computing services may provide access to solid web platforms and data storage through public electronic communications network. It also encourages information sharing, a fundamental feature for STD. For example, a sophisticated tour guide system could serve massive number of tourists without being actually installed on any personal device, even allowing personalizing experiences;
ii.) Built on an infrastructure of state-of-the-art technology, «[…] accessible to everyone, which facilitates the visitor's interaction with and integration into his or her surroundings, increases the quality of the experience at the destination, and improves residents' quality of life»[14];
iii.) Smart business networks, referring to the number of applications at various levels supported by a combination of Cloud Computing and IoT.

2.2 Technology-Enhanced and Empowered Experiences

The shared purpose of all omni-channel actors of a smart tourism ecosystem is to provide enhanced/enriched, high-value, meaningful, memorable tourism experiences through services and products mediated through technology (technology-mediated experiences).
Such experiences are rendered enhanced or empowered, according to the type and role of technology used. In technology-enhanced experiences, technology available in the Web 2.0 plays a supporting role to make consumers actively participate and shape the creation of their experiences. Consumers use social networking sites and mobile apps to interact with organizations, use review sites, comment and use media to share their experiences[15].
On the other hand, "technology-empowered experiences" emerge from advanced technological developments, such as interactive environments, augmented reality, near field communications, gaming, etc. At this latter level, technology is pervasive and allows tourists to interact and engage with the different service-providers throughout all the stages of travel, service encounters and touch-points, either in the physical tourism destination or in the online space. These new experiences are predicted to be richer, more participatory. In fact, consumers play an active part in co-creating[16] their own experiences, recognizing these way active consumers co-creating their experiences in a quest for personal growth and value.
It is pertinent to systematize and explore some types of technologies worn in practical

[14] M. Höjer – J. Wangel, *op. cit.*

[15] L. Tussyadiah - D. Fesenmaier, *Mediating the tourist experiences access to places via shared videos*, in *Annals of Tourism Research*, vol. 36, issue 1, 2009, 24 ss.

[16] C.K. Prahaland – V. Ramaswamy, *Co-creation experiences: the next practice in value creation*, in *Journal of Interactive Marketing,* vol. 18, issue 3, 2004, 5 ss.

settings within destinations to enhance and empower experiences. Technologies range from:

- Social networking sites (SNSs);
- Mobile applications (destination apps);
- Interactive websites;
- Interactive ordering systems (eTable technology);
- Interactive mobile platforms (iPads);
- Wearable devices;
- Big data analytics;

Social networking sites (SNSs), as referred in i., have already expanded their capabilities as build-in apps to meet social media user´s needs; they are mostly Facebook, YouTube, Twitter, TripAdvisor, Yelp and have made user-generated content (UGC) such as preferences, needs, interests, profiles, etc. freely accessible online. Such user-input content is reified in social profiles, reviews, ratings, comments, impressions on past experiences, recommendations for future purchases, etc.). The travel review website TripAdvisor generates a significant source of tourism-related (open) data given the figures and reviews on attractions/destinations; as a means of illustration, «in 2015, TripAdvisor reached 320 million reviews and had 6.2million opinions on places to stay, to eat and on things to do - including 995,000 hotels and forms of accommodation, 770,000 vacation rentals, 3.8 million restaurants and 625,000 attractions in 125,000 destinations throughout the world»[17].

Destination mobile applications mentioned in ii. are characterized by their "*mobiquity*" (mobility and ubiquity), and free wifi access to information anywhere and anytime have led to a behavioral transformation of tourists from *"sit and search" to "roam and receive"*[18].

As an example of iii., the interactive online website *PixMeAway*[19] is a picture-based search engine that allows consumers to interact with the interface, select appealing travel motifs, photos, the traveler type, and define their travel personality. The website will provide destination suggestions matching their criteria.

As an example of iv. the Inamo Restaurant[20] provides an instance in which the technology empowers the tourism experience. This restaurant «[…] introduces a fully digitalized dining experience and interactive ordering system. This system, developed by E-Table, uses a combination of table touchpads and overhead projection to allow customers to see the food and drinks menu projected onto the table surface. The system further allows customers to change table clothes to the current mood and preferences, watch their food being prepared in the kitchen through a webcam in real time, manage the waiter and bills, explore the local neighborhood for activities afterwards or order a cab home. By doing so, the restaurant provides the physical technology (interactive

[17] E. Pantano – C.V. Priporas et al., *You will like it!' Using open data to predict tourists' responses to a tourist attraction*, in *Tourism Management*, vol. 60, 2017, 430 ss.; and also the *TripAdvisor annual report for 2015*, accessible online.

[18] M. Pihlström, *Perceived Value of Mobile Service Use and its Consequences*, Helsinki, Swedish School of Economics and Business Administration, 2008, accessible online.

[19] Accessible online.

[20] Accessible online.

tables) without which the unique dining experience could not occur, rendering the technology the central element of the experience creation».

As an example of v., the Hotel Lugano Dante[21] provides a case of hotel enrichment context where mobile platforms can come into play to facilitate and enhance the level of interaction between company and guests throughout the entire hotel experience. In such hotel, «Guests provide personal information and preferences, such as room temperature, favorite beverages, and preferred newspapers and so on, whereas members of staff retrieve this specific information. By accessing the platform on a mobile device, the hotel and guests co-create through exchanging information in real time, which are used to facilitate encounters on multiple touch points. This leads to more personalized interactions, more valuable service encounters and on overall enhanced experience for the guest».

Wearable devices, listed as vi. are body-attached computers and are part of the IoT, therefore contributing to ubiquitous computing. Nowadays, there are different types of wearables applied to tourism destinations[22]:

- Smart watches provide notifications such as status updates, comments, photo tags, check-in, etc. Tourists can also receive real-time flight alerts, gate changes, and other information on their wrists;
- Bracelets/watches can track guests' sleeping patterns, as clients wear a watch while sleeping and wake them through gentle vibrations;
- Wrist band able to swipe hotel room keys;
- Smart glasses used by tourists in museums, art galleries to see cultural artifacts and activate digital contents, such as video, games, photos, etc. on the glass display screen by simply looking at the collection item; visitors can easily switch between real objects and augmented reality.

All wearables have in common the fact they collect and process user-specific data. Alongside body-data, many wearables record location-data and geo-data, often unnoticed by the users, for they can be used to calculate the distance travelled, to determine the user's location, etc., which poses a challenge for present data protection and privacy. Moreover, the use of wearable devices does not only involve its user (the owner of the device), but also the manufacturer, third-party providers and other intermediaries (insurance companies, scientists or advertising companies). Furthering, data is often not stored locally or processed by the device itself, but forwarded to a Cloud service (even possibly located outside Europe)[23].

Concerning big data analytics, pointed in vii., tourism data is an asset being exploited using a multi-modal pipeline of advanced data analysis methods called big data analytics[24] comprising content analytics crawlers (mining unstructured content), machine

[21] B. Neuhofer - D. Buhalis et al., *op. cit.*

[22] R. Atembe, *The Use of Smart Technology in Tourism: Evidence From Wearable Devices*, in *Journal of Tourism and Hospitality Management*, vol. 3, n. 11-12, 2015, 224 ss.

[23] T. Jülicher – M. Delisle, *Step into 'the circle'—a close look at wearables and quantified self*, in T. Hoeren – B. Kolany-Raiser (eds.), *Big data in context - legal, social and technological insights*, Heidelberg, 2018, 81 ss.

[24] K. Waterman – P. Bruening, *Big data analytics: risks and responsibilities,* in *International data privacy law*, vol. 4, issue 2, 2014, 89 ss.

learning (ML) algorithms, natural language processing tools (NLP) and data mining techniques (DM). Distinctive aspects of big data analytics are briefly mentioned herewith to foresee its implications on data protection[25]: i. Use of large numbers of ML algorithms against data to find correlations, inferences between data. Once relevant correlations are identified (originally unforeseen), a new ML algorithm can be created and deployed to specific cases in the future; ii. Tendency to collect and analyze *all* the data that is available; iii. Repurposing of data for which it was originally collected, as analytics can mine data for new insights and find correlations between apparently disparate datasets; and iv. Use of new types of data automatically generated and coming from the IOT devices, as sensors. Even though these methods endow stakeholders with a fine-grained data to extract value, trends and patterns, thereby enabling them to customize technology-empowered experiences through smart products and services, they also increase known risks hampering privacy and data protection[26].

The implementation of the above mentioned smart ICT enhances tourism experience through the offer of products/services that are customized, personalized (personalized infotainment services), to meet each of the visitor's unique needs and even implied desires, since understanding travelers' needs, wishes and desires becomes increasingly critical for the attractiveness of destinations. Such customization, personalization and profiling is attained by *collecting* UGC from all these technological artifacts, and *reusing* it to provide meaningful offers fitting perfectly the clients' needs[27] with the ultimate desideratum of achieving more satisfaction[28] at the experience environment.

Therefore, tourism-related data has multiplied geometrically[29] through its varied provenance (SNSs, apps, sensors, etc.). These sources provide a massive size of volunteered, observed, inferred or collected digital traces, resulting in multidimensional sets of data, known as big data[30]. This massification of real-time tourism-related data, analyzed by IoT industries, has created big pools of data to mine. Hence, SDT can be considered both as consumers and producers of big data.

This tourism-related data, inherently cross-border, holds strategic commercial value. It comprises, for example, i. transactional data between tourists and transportation/hospitality undertakings (airlines, hotel, restaurants and rental car businesses)[31] derived

---

[25] A. Mantelero – G. Vaciago, *The 'dark side' of big data: private and public interaction in social surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds in social surveillance,* in *Computer law review international*, vol. 14, 2013, 161 ss.

[26] H. Couturier, *At the big data crossroads: turning towards a smarter travel experience*, Amadeus IT group report, 2013, accessible online.

[27] L. Edwards, *Privacy, security and data protection in smart cities: a critical EU law perspective*, in *European data protection law review*, vol. 2, 2016, 28 ss.

[28] R. Law – R. Leung et al., *Information technology applications in hospitality and tourism: a review of publications from 2005 to 2007*, in *Journal of travel & tourism marketing*, vol. 26, issue 5-6, 2009, 599 ss.

[29] J. Manyika – M. Chui et al., *Big data: the next frontier for innovation, competition, and productivity*, Report McKinsey Global Institute, 2011, accessible online.

[30] B. Habegger – O. Hasan et al., *Personalization vs. Privacy in Big Data Analysis*, in *International Journal of Big Data*, issue 1, 2014, 25 ss.

[31] These activities reveal aspects on destination/origins, way-finding preferences (beach, sports, culture, restaurants, etc.), spending capacities, and on behaviors (family tourism, leisure, night clubs, events, etc.), etc.

from queries/searches, purchases, and other exchanges; ii. geographical data; and iii. UGC from client's profiles, established preferences, needs, etc. These data can reveal commercial preferences of its users, allows the detection and prediction of future behaviors and trends, rendering enormous interest for economic operators, and allow destinations to better plan for future tourists in terms of mobility, popular attractions, and other potential issues. By managing such big data, tourism organizations can extract valuable insight from information that could elevate them to a new dimension of customer experience and improve the way they interact with customers, hence gaining competitive advantage[32]. Such information is the fabric for companies to convert big and open data[33] into future preferences and value propositions[34].
However, such processing of personal information (data trails or digital footprints) contains the risk of building of a detailed profile of tourists, actually, a holistic personal mosaic of the individual users, with imminent implications for privacy and data protection[35].

3. Compliance of Smart Tourism Destinations with the privacy and data protection principles

3.1. Fairness and Transparency

Article 5(1) (a) states that personal data must be «processed fairly, lawfully and in a transparent manner in relation to the data subject». Accordingly, destinations must assess if their processing of personal data is fair and transparent. Transparency of automated decision-making is taking an increasingly important role with the advent of big data analytics. Whether the data are volunteered, observed, or inferred, or collected from accessible sources, individuals are fully entitled to know which are they, from where and from whom the controllers obtained it, and how automated decisions were taken. Denote that big data algorithms (also used in STD scenarios) learn and change in a (semi) autonomous way, making them hard to document; further, organisations often claim secrecy over "how" data is processed on grounds of commercial confidentiality and copyright protecting the software and the trade-secret shield[36]. Profiling and cor-

[32] D. Buhalis – A. Maranggana, *op. cit.*

[33] We denominate this data as "open data", as it accomplishes the criteria of i. availability and access; ii. reuse and redistribution; iii. Universal participation, i.e., this data can be reused by anyone, https://okfn.org/opendata/. It is notable to state that growing amount of tourism-related open data is available in machine-readable ways (XML, CSV, or JSON format), E. Pantano – C.V. Priporas et al., *op. cit.*

[34] M.D. Masseno, *On the relevance of Big Data for the formation of contracts regarding package tours or linked travel arrangements, according to the New Package Travel Directive*, in *Comparazione e diritto civile*, 4, 2016, 2 ss.

[35] I. Rubinstein, *Big Data: The End of Privacy or a New Beginning*, in *International Data Privacy Law*, vol 3, issue 2, 2013, 74 ss.; also, R. Kemp, *Legal aspects of managing big data*, in *Computer Law and Security Review*, vol. 30, 2014, 482 ss.

[36] P. Schwartz – D. Solove, *The pii problem: privacy and a new concept of personally identifiable information*,in *New York University Law Review*, vol. 86, 2011, 1814 ss.

relation results are hence invisible and opaque, and its results often impenetrable to laymen. Secret-tracking and decision-making on the basis of profiles are then hidden from any consumer-tourist, which is left without meaningful information about the employed "algorithmic logic". Still, we are attentive to a right to know the "logic of the processing" applied to data (Recital 63, and Arts. 13(2) (f), and 15(1) (h)), respectively.
The GDPR defines profiling in Article 4 as: «[…] any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements».
Profiling is an important feature in tourism destinations. Tourism service providers are adapting their serviceable approach to meet the personalization expectation[37]. In fact, data-processing scenarios collect user's input and feedback which are used to build fine-grained premium services and recommender systems in the form of trail packages. The richer the user profile, the higher the temptation for the operators to target a user with unsolicited advertising or to engineer a pricing structure capable to extract as much surplus from the user as possible[38].
The GDPR prohibits automated individual decision-making that significantly affect individuals, Art. 22 (1). Notably, «[…] analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behavior patterns».[39]
Indeed, developments on consumer-tourist automated profiles, facilitated by big data analytics, can *significantly affect* data subjects[40]. Covert profiling can, in certain cases, lead to unintended consequences:
i. when based on incomplete data, profiling can lead to false negatives, depriving individuals from benefits that they would be entitled to;
ii. "*filter bubbles*" effect[41], according to which data subjects will only be exposed to content which confirms their own preferences and patterns, without any door open to serendipity and casual discovery;
iii. isolation and/or discrimination, e.g., including price differentiation, without providing the individuals the possibility to contest these decisions. In a STD, ML decisions and profiling can lead to promote direct or indirect discrimination decisions through the exclusion/denial of services/goods, e.g. denial of insurances, exclusion from the sale of touristic services or high-end products, shops or entertainment complexes to certain profiled tourists and even other decisions that reflect upon health, creditworthiness, recruitment, insurance risk, etc; it even can lead to discriminate essential utilities for those unwilling to share personal data[42]. In this synopsis, tourists might be

37 L. Edwards, *op. cit.*

38 ENISA 2015 report, *Privacy and data protection by design – from policy to engineering.*

39 Art. 29 WP, Opinion 8/2014, *Recent developments on the Internet of Things.*

40 EDPS, Opinion 3/2015, *Europe's big opportunity*, *EDPS recommendations on the EU's options for data protection reform.*

41 E. Pariser, *The filter bubble: what the Internet is hiding from you*, New York, 2011.

42 P Schwartz – D. Solove, *op. cit.*

discriminated against because they belong to a particular social group, but also, such ascertainment might be based on factors, identified by the analytics, that they share with members of that group.
Therefore, in order to ensure a fair and transparent processing, automated decisions should account all the circumstances concerning the data and not be based on merely de-contextualized information or on data processing results.
In furtherance of this aim, the controller should find ways to build discrimination detection into their ML systems, to prevent inaccuracies and errors assigned to labeled profiles; as referred in Recital 71, the controller should «[…] use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect».

3.2. Lawfulness of Processing: Consent, Legitimate Interests, Contract and Public sector

In this sort of intelligent environment, it is dubious to give or withhold our prior consent to data collection[43], as it seems to be absent by design. The awareness that the ubiquitous sensors are so embedded in the destination that they literally "disappear" from the users' sight, so that they will not even be conscious of their presence and hence consent to the collection, can be envisaged within STD. We can, at some extent, concede that the obtaining of such consent, in STD contexts, would be defined in a mechanical or perfunctory manner, or as a "routinization".
We note also that as for CCTV, ANPR and MAC whilst tracking and sensing, the notice in the form of information signs in the area being surveilled, or on related websites, does not conform to the consent requirements. The issue of the IoT embedded in STD is that its sensorization devices are explicitly designed to be unobtrusive and seamless, invisible in use and unperceived to users[44] and thereupon, users do not hold the opportunity give their unambiguous, informed, specific, explicit, and granular consent[45]-[46]. Therefore, the data controller might have difficulty in demonstrating that the

[43] R. Kitchin, *Getting smarter about smart cities: Improving data privacy and data security*, Data Protection Unit, Department of the Taoiseach, Dublin, 2016.

[44] P. Schwartz - D. Solove, *op. cit.*

[45] Art. 29 WP, Opinion 15/2011, *Definition of Consent*; Art. 29 WP (259 rev. 01), *Guidelines on Consent under Regulation 2016/679*.

[46] A. Mantelero, *The future of consumer data protection in the E.U. Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics*, in *Computer Law and Security Review*, vol 30, 2014, 643 ss.

consent was given, and the data subject is not able to withdraw that consent[47].
Still, consent is not yet part of a function specification of IoT devices, and thus, they do not have means to display «provide fine-tuned consent in line with the preferences expressed by individuals» because smart roads, trams, tourist office devices are usually small, screenless and lack an input mechanism (a keyboard or a touch screen)[48].
Regarding the amount and assortment of these interactions, it is just too onerous for each data subject to assess their privacy settings across dozens of entities, if any, in order to ponder about the non-negotiable tradeoffs of agreeing to privacy policies without knowing how the data might be used now and in the future, and to assess the cumulative effects of their data being merged with other datasets[49].
Reverting also to other legal grounds, processing personal data relies on "public interest", which can sidestep the need for consent (health, national governmental agencies gather data for e. g. e-Government systems, e-Health). Nevertheless, this possibility should not conceal any eventual "third-party interest".
Most commercial systems rely on the "legitimate interests" ground, even if they consist in «the vaguest ground for processing»[50], and offers a lot of scope for industry to process data by claiming any deemed necessary "legitimate interest". In fact, the processing must be "necessary" for the legitimate interests and not just *potentially* interesting[51]. It follows that the processing is not necessary if there is any other way of meeting the legitimate interest that interferes less with the people's privacy[52]. Implicitly, the task of balancing commercial interests and user fundamental rights [53] is delegated to the controllers themselves[54].
As for the contractual condition, it may be difficult to show that big data analytics in STD are strictly necessary for the performance of a contract, since the processing goes beyond what is required to sell a product or deliver a service.

3.3. Purpose Limitation

This principle utters that the purpose for which the data is collected must be specified and lawful, Art. 5(1) (b). This principle also prevents arbitrary reuse[55], calling for a «compatibility assessment of the new purpose»[56]. As for a repurpose, personal data should not be further processed in a way that the data subject might consider

47 E. Carolan, *The continuing problems with online consent under the EU's emerging data protection principles*, in *Computer Law and Security Review*, vol. 32, issue 3, 2016, 462 ss.

48 Art. 29 WP, Opinion 8/2014, *Recent developments on the Internet of Things*.

49 B. Habegger – O. Hasan et al., *op. cit.*

50 EP Study, Big *Data and Smart Devices and their Impact on Privacy* (2015).

51 ICO, *Big Data*, *Artificial Intelligence, Machine Learning and Data Protection*, UK, 2017.

52 Art. 29 WP, Opinion 06/2014, *Notion of legitimate interests of the data controller.*

53 EDPS, Opinion 7/2015, *Meeting the challenges of big data.*

54 P. Schwartz - D. Solove, *op. cit.*

55 Art. 29 WP, Opinion 03/2013, *Purpose Limitation*, 21.

56 ICO, *Big Data, Artificial Intelligence,* cit.

unexpected, inappropriate or otherwise objectionable[57] and therefore unconnected to the delivery of the service; concretizing, by exposing data subjects to different/greater risks than those contemplated by the initial purposes could be considered as a case of further processing of data in an unexpected manner.
In what refers the compatibility assessment, Article 29 WP states that «By providing that any further processing is authorized as long as it is not incompatible […], it would appear that the legislators intended to give some flexibility with regard to further use. Such further use may fit closely with the initial purpose or be different. The fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis». This Opinion sets out an approach to assessing whether any further processing is for an incompatible purpose. Moreover, Recital 50 of the GDPR states that in assessing compatibility it is necessary to take account of any link between the original and the new processing, the reasonable expectations of the data subjects, the nature of the data, the consequences of the further processing, and the existence of safeguards.
Yet, automatic capture of tourism data through sensors might be collected for potentially secondary unauthorized purposes that had not been initially scheduled or still to be discovered, or for profiling, for abusive marketing activity, undermining this way the purpose limitation principle.
Anyway, in practical settings, companies «[…] repackage data by de-identifying them (using pseudonyms or aggregation) or creating derived data, with only the original dataset being subjected to data minimization. The repackaged data can then be sold on and repurposed in a plethora of ways that have little to do with the original reason for data generation and without the need to give notice or consent to those that the data concerns»[58].

3.4. Data Minimization: Collection and Retention

The GDPR says personal data shall be «[…] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed», Art. 5 (1) (c), and so organizations should minimize the amount of data they collect and process, and the length of time they keep the data.
Yet, in substance, smart technology purports the massive collection, aggregation and algorithmic analysis of all the available for various reasons, such as understanding customer buying behaviors and patterns or remarketing based on intelligent analytics. Big data analytics may discover unexpected correlations that do not retrospectively justify obtaining the data in the first place, for example, between data about people's lifestyles and their credit worthiness. Therefore, organizations need to be clear about which data is deemed to be *necessary, excessive* and *relevant* for the purposes of the pro-

[57] Council of Europe Guidelines, *Protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD, 2017.

[58] D. Solove, *I've Got Nothing to Hide and Other Misunderstandings of Privacy*, in *San Diego Law Review*, vol. 44, 2017, 745 ss.

cessing.
In addition, personal data shall not be kept longer than necessary for the purpose for which it is being processed, as prescribed by the storage limitation principle, Art. 5 (1) (e). This principle is becoming part of the lifecycle governance strategy retention policies of companies that defensibly dispose irrelevant data instead of keeping data archived forever. Retention schedules allow unnecessary data to be disposed of as it is no longer of business value or needed to meet legal obligations.

3.5. Accuracy and Up-to-date Processing

Results drawn from big data analysis may not always be representative or accurate as sought (Art. 5 (1) (d)), if sources aren´t accurate as well (*i.*e. analysis based on social media resources are not necessarily representative of the whole population at stake) [59].
Organizations employing ML algorithms to discover associations need to consider the distinction between correlations and causations[60], *i.e.*, when there is no *direct cause and effect* between two phenomena that show a close correlation. In these cases there is a risk of drawing inaccurate, but also – and when applied at the individual strata – potentially unfair and discriminatory conclusions[61]. The potential accuracy (or inaccuracy) of any resulting decisions might cause discriminatory, erroneous and unjustified decisions, regarding data subject´s behavior on health, creditworthiness, recruitment, insurance risk, etc..
Even exercising the "right to be forgotten" (Art. 17), where data subjects will have the right for their data to be erased in several situations, for e.g., when the data is no longer necessary for the purpose for which it was collected, or based on inaccurate data, it may be difficult for a business to find and erase someone's data if it is stored across several different systems and jurisdictions[62].
Further, inaccuracy of data endangers the data quality principle and triggers abstract strict liability for damage[63].
The quality of the profiles and the quality of personal data on which they are built, again, seem to matter for the prosperity of the industry, yet another relevant privacy principle.

4. Reflections and Conclusions

This study is novel in having undertaken an initial exploration of the legal implications

[59] ICO, *Big Data, Artificial Intelligence,* cit..

[60] *Ibidem*

[61] EDPS, Opinion 7/2015, *Meeting the challenges of big data.*

[62] C. Bartolini – L. Siry, *The right to be forgotten in the light of the consent of the data subject*, in *Computer Law and Security Review*, vol. 32, 2016, 218 ss.

[63] T. Hoeren, *Big Data and Data Quality*, in T. Hoeren – B. Kolany-Raiser (eds.), *Big Data in Context - Legal, Social and Technological Insights*, Heilderberg, 2018, 1 ss.

that technology-enhanced (and empowered) tourism experiences imply to data protection and privacy. The preceding analysis brings out that smart tourism is becoming a big contributor and benefactor of ubiquitous, always-on data-capture about consumer-tourists towards empowered tourism experiences and competitive markets. This data allows the detection and prediction of future behaviors and trends; allows the analysis of development and optimization processes of products/services, retention of customers, and ultimately is useful for future decision-making.

Patently, with new forms of ICTs emerging over the coming years, more types of technology-empowered experiences are expected to flourish further and trigger new challenges to the body of tourism knowledge and wariness therewith.

As for now, the current assumption is that all captured information is extremely valuable and necessary to organizations and will be freely provided by the smart tourists who seek enriched tourism experiences[64].

This extensive collection and processing of personal data in the context of smart tourism destinations using algorithm-driven techniques has given rise to serious privacy concerns, especially relating to the wide ranging electronic surveillance, profiling, and disclosure of private data.

Moreover, the lack of privacy and data protection mindset of engineers and coders working in IoT/cloud business poses a very large problem for the future[65].

In this line, smart technologies used in STD often produce situations of imbalance, where data subjects are not aware of the fundamental elements of data processing and related consequences, being unable to negotiate their information, which leads to a side effect of enhanced information asymmetry[66].

Information asymmetry and inadequate provision of information and data sharing to the public about data use can be seen as hampering tourist trust in STD.

This scenario is particularly acute with "digital natives" or "*millennials*" tourists who have grown up with ubiquitous internet access and share willingness personal information via social media with fewer concerns for how it may be used.

Smart tourism raises big issues with respect to information governance[67] and about correctly deriving the *added* value from information in an open and ubiquitous info-structure. The apprehension here is to understand if the affordances of the technology, the personalized services, and empowered experiences can cope with data protection obligations without a micro-targeting and profiling for unintended uses, safeguarding the right to equal treatment, to non-discrimination and the protection of personal autonomy based on a person's right to control his/ her personal data, that may never be the price paid for an enhanced awareness.

---

64 P. Tallon, *Corporate governance of big data: perspectives on value, risk, and cost,* in *Computer*, vol. 46, issue 6, 2013, 32 ss.

65 P. Schwartz - D. Solove, *op. cit.*

66 M.D. Masseno, *Personal data circulation from the EU to USA and now what for the American Tourism Industry with business in Europe*?, 23rd International Tourism Safety Conference, Las Vegas, 2016.

67 I. Hadar – T. Hasson et al., *Privacy by designers: software developers' privacy mindset*, in *Empirical Software Engineering*, vol. 23, issue 1, 2018, 259 ss.

In the forthcoming future, controllers should adopt a precautionary approach[68] in regulating data protection in this field of STD, such as adoption of compliance tools enable STD organizations meeting their data protection obligations while protecting people's privacy rights in a STD context, and they are: anonymization and pseudonymization techniques, privacy policies, data protection impact assessment (DPIA), personal data stores, algorithmic transparency, privacy seals/certification, and privacy by design measures to mitigate the appointed legal risks and implications. It is suggested that STD are to proceed with test prototyping and research before the implementation of new technologies and services in large-scale real-life environments, such as the Mobile Living Lab[69].

As future work, besides addressing related information security issues according to the NIS Directive[70], future research regarding mobile devices and tracking will be needed, following the adoption of the new *ePrivacy* Regulation[71], as well as qualifying the roles of data controller and data processer in the context of STD. Besides, as stated in the Tourism Science literature, tourism, by definition, is a service-intense industry with a "business network", since it relies on a number of stakeholders for its ability to deliver products and services[72]. Hence, the term *business network* refers to «[…] a collection of inter firm relationships, including alliances, long-term buyer-supplier relationships, and informal collaborations» where each of the actors involved process personal data and therefore their legal obligations should abide to the GDPR.

[68] ICO, *Big Data, Artificial Intelligence,* cit.

[69] L. Edwards, *op. cit.*

[70] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[71] Proposal of a Regulation of the EP and of the Council concerning the respect for private life and the protection of personal data in electronic communications, COM/2017/010 final - 2017/03 (COD).

[72] P. Robertson, *An Assessment of Collaborative Governance in a Network for Sustainable Tourism: The Case of RedeTuris*, in *International Journal of Public Administration*, vol. 34, issue 5, 2011, 279 ss.