SMART TOURISM DESTINATIONS PRIVACY RISKS ON DATA PROTECTION– A FIRST APPROACH, FROM AN EUROPEAN PERSPECTIVE[1] [2]

Manuel David MASSENO[3]

Cristiana SANTOS[4]

ABSTRACT: Tourism-related data created by tourists and processed in a smart tourism environment concern mostly personal data deriving from diverse sources: social networks, intelligent apps, ubiquitous sensors, big data analytics, etc., providing a massive size of volunteered, observed, inferred or collected digital traces, resulting in multidimensional sets of available and accessible data, at least for its controllers. Such data is the fabric for organizations to convert tourism information into future preferences and value propositions of empowered tourism experiences, ready to be monetarized. Therefore, the exploitation of data related to this perceived enjoyment must be considered in the legal framework of data protection by exposing potential risks to data protection and privacy, along with the available compliance tools, namely those provided by the New GDPR. In short, Smart Tourism Destinations are one of the best available benchmarks regarding data protection regulations.

KEYWORDS. Privacy and Data Protection, Smart Tourism Destinations, EU Law, Intelligent Environments, Fundamental Rights

RESUMO. Os dados relacionados com o Turismo criados pelos turistas e tratados em meios ambientes inteligentes consistem sobretudo em dados pessoais cuja origem provém de diversas fontes: redes sociais, aplicativosinteligentes, sensores ubíquos, analíticas de megadados, etc., fornecendo registros digitais facultados, observados, inferidos e obtidos numa escala massiva, dando lugar a conjuntos multidimensionais de dados disponíveis e acessíveis, pelo menos para quem os trata. Tais dados são a matéria usada pelas organizações para

[1] Artigo elaborado no âmbito do Projeto de Pesquisa: "*Big Data*, *Cloud Computing* y otros retos jurídicos planteados por las tecnologias emergentes; en particular, su incidencia en el sector turístico" - DER2015- 63595 (MINECO/FEDER), Coordenado pela Professora Apollònia Martínez Nadal, Catedrática da *Universitat de les IllesBalears*, Espanha.

[2] Este artigo assenta no texto aprovado (dupla revisão anônima por pares) para a Oficina / Workshop: Legal Issues in Intelligent Environments'18 / 14th International Conferenceon Intelligent Environments- IE'18, Universidade 'La Sapienza', Roma, a ter lugar a 26 de junho de 2018.

[3] Professor Adjunto de Graduação e Mestrado e Pesquisador Sênior no Laboratório UbiNET - Segurança Informática e Cibercrime do Instituto Politécnico de Beja, Portugal. No Brasil, além de integrar o Grupo de Trabalho de Direito Digital e Compliance da FIESP – Federação das Indústrias do Estado de São Paulo, é Consultor das Comissões de Direito Digital e Compliance de Legislação Aplicada à Hotelaria e ao Turismo da OAB São Paulo.

[4] Mestre em Direito dos Contratos e da Empresa, pela Universidade do Minho, Portugal. Doutorada em Direito e Tecnologia e em Informática Jurídica pelo Programa de Doutoramento Erasmus Mundus - JointInternationalDoctoralDegree em "Law, ScienceandTechnology" (Universidades de Bolonha, de Turim, Autónoma de Barcelona, MykolasRomeris de Vilnius, do Luxemburgo e de Tilburgo). Pesquisadora no JusGov - Centro de Investigação sobre Justiça e Governação da Escola de Direito da Universidade do Minho.

converter as informações turísticas em futuras preferências e propostas de valor para experiências turísticas reforçadas, prontas a serem monetarizadas. Consequentemente, a exploração dos dados relacionados com estas satisfações acrescidas precisa de ser considerada no âmbito jurídico da proteção de dados, pondo em evidência os riscos potenciais para a privacidade e a proteção de dados, justamente com as ferramentas disponíveis para efetivar o respetivocumprimento, designadamente as facultadas pelo Novo RGPD – Regulamento Geral sobre Proteção de Dados da União Europeia. Em suma, os Destinos Turísticos Inteligentes são um dos melhores critérios para testar as regulações relativas à proteção de dados

PALAVRAS-CHAVE. Privacidade e Proteção de Dados, Destinos Turísticos Inteligentes, Direito da União Europeia, Meios Ambientes Inteligentes, Direitos Fundamentais

Introduction

Smart Tourism Destinations(hereinafter called STD) emerge from the technological foundations of *Smart Cities*, themselves 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 interaction and legal consequences at 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 (ANUAR, F.I.; GRETZEL, U., 2011; BUHALIS, D.; AMARANGGANA, A., 2014; and GRETZEL, U.; SIGALA, M., 2015), being this paper a sort of primer endeavor.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.

With technology being embedded within destinations environments, addressing the potential needs and desires even at an unconscious level of travelers, STD are designed for enriching those experiences and to enhancethe competitiveness of each destination.Regarding the connection between Tourism and ICT, we're facing a specific context, where the relationship of clients with providers through their apps/services is generally short-lived, which makes trust-building, as costumer'sloyalty, much harder (NEUHOFER, Barbara *et al.*, 2015). Moreover, the need for real-time information *in situ* is so imminent that tourists might be easily persuaded to forego their data. On another hand, benefits or"*perceived enjoyment*" (evoked by engaging content and interactive system features) are heightened (GRETZEL, U.; SIGALA, M.*et al.*, 2015), suggesting that personal data and privacy concerns might be suspended. At the same time, 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 risk perceptions and therefore personal data and privacy concerns (ANUAR, F.I.; GRETZEL, U., 2011; and, BUHALIS, D.; AMARANGANNA, A., 2015).Nevertheless, these risks are amplified as the number of connected smart objects grows and are multiplied by the complexities involved in multiple vendors and interoperating systems.

A few illustrative examples may provide insight towardspossible personalized and smart value-added services STD can offer, as full historic or environmental immersions through smart optics devices or augmented reality. Further, location-based services could alert users on promotional offers in restaurants that are close to them at any given time. Besides, estimated waiting time in restaurants can be accurately quoted, to the minute, so guests can get a drink in the bar while waiting for their table. 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. RFID tags on the luggage during check-in, to make it easier to locate the luggage after the plane lands in the destination, is also configured in STD scenarios. All this allows tourists to get much more from their travel and helps fulfilling the experiential travelling potential of the destination (BUHALIS, D.; AMARANGANNA, A., 2014).So, as pointed out by Tourism Science literature, privacy and data protection research is needed in the Tourism context, balancing the trade off value and affordances added by STD and its legal protection.

The paper is organized as follows. Section 1 refers to the background of STD, describing the specificities of a smart destination and the embedded technologies used to conceive enhanced and empowered experiences for tourists. Section 2 provides some of the most important risks that can be appointed to STD regarding privacy and data protection, and its corresponding compliance tools depicted in the GDPR - General Data Protection Regulation of the European Union (Regulation (EU) 2016/679), as the current basis of the Privacy and Data Protection Legal system in the European Union. Section 3 concludes the paper and provides some clues for future directions.

1. Smart Tourism Destinations

This section aims to describe the constituents of STD, its objectives, and the intersection of tourism dimensions with technology mediated experiences: enhanced and empowered experiences that tourist can enjoyin practical settings within destinations. It also intends to explain the types and the sources of tourism data and substantiate the strategic commercial value of tourism data.

1.1. Smart Tourism Destinations

In order to characterize the functions layered on tourism destinations, it is worthy to point out that successful destinations are composed by five dimensions: transportation, accommodation, gastronomy, attractions and ancillaries services, which can be then structured into six axes or "6As" as the literature describes (BUHALIS, D., 2000), 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, as created by tour operators; v. Activities; and vi. Ancillary Services (e.g. daily use services such as bank, postal and health services).

By adding*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. (GRETZEL, Ulrike; REINO, Sofia *et al*., 2015).

This embracing concept comprises three core elements (HÖJER, M.; WANGEL, J., 2015):

i. Reliance on smart technology infrastructures, wireless sensor networks (*IoT*) and integrated communications systems, e.g. sensor technology, ubiquitous Wi-Fi, 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 (GRETZEL, Ulrike; REINO, Sofia *et al*., 2015). *IoT* provides support in terms of 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; namely, a sophisticated tour guide system could serve massive number of tourists without being installed on any personal device, even allowing personalized 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. (GRETZEL, U.; SIGALA, M. *et al*., 2015).

iii. Smart business networks, referring to the number of applications at various levels supported by a combination of *Cloud Computing* and *IoT*.

1.2. 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 by services and products that are 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. Therefore, consumers use social networking sites (SNSs) and mobile apps to interact with organizations, use review sites, comment and use media to share their experiences (TUSSYADIAH, L.; FESENMAIER, D., 2009).

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-creatingtheir own experiences, recognizing these way active consumers co-creating their experiences in a quest for personal growth and value (PRAHALAND, C. K.; RAMASWAMY, V., 2004).

So, it's necessary to systematize and explore some of the technologies worn in practical settings to enhance and empower these experiences. Technologies that range from: i. social networking sites (SNSs); ii. mobile applications (destination apps); iii. interactive websites; iv. interactive ordering systems (*eTable technology*); v. interactive mobile platforms (iPads); vi. wearable devices; and vii. big data analytics;

1.2.1. Social networking sites (SNSs)

Referred in i., *SNSs*have already expanded their capabilities as build-in apps to meet social media user´s needs; the most relevant are *Facebook, YouTube, Twitter,* or comparative services, such as *TripAdvisor, Yelp*, *Booking.com*, 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, satisfaction surveys, reviews, ratings, comments, impressions on past experiences, recommendations for future purchases, etc.(PANTANO, E.*et al*., 2017). Namely, 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[5].

[5] The*TripAdvisor annual report for 2015,* accessible at http://ir.tripadvisor.com/static-files/a0cc5025-7f78-416f-9643-e863f5e307a5, consulted on 20/05/2018.

1.2.2. Destination mobile applications

These, as mentioned in ii., are characterized by their "*mobiquity*" (mobility and ubiquity), and free Wi-Fi access to information anywhere and anytime have led to a behavioral transformation of tourists from "*sit and search*" *to* "*roam and receive*"(PIHLSTRÖM, M., 2008).

1.2.3. Interactive Websites

As an example of iii.,we may point out the interactive online website *PixMeAway*[i6], 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 theircriteria.

1.2.4. Interactive ordering systems

For iv, *Inamo Restaurant*[7] provides an instance in which the technology empowers the tourism experience, as it:

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

1.2.5. Interactive mobile platforms

As an illustration of v., the *Hotel Lugano Dante* 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 hospitality experience, as:

> Guests provide personal information and preferences, such as room temperature, favorite beverages, and preferred newspapers and so on,

[6] Accessible at http://www.pixmeaway.com/, consulted on the 20/05/2018.

[7] Accessible at http://www.inamo-restaurant.com/, consulted on the 20/05/2018.

> 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 tofacilitate encounters on multiple touch points. This leadsto more personalized interactions, more valuable service encounters and on overall enhanced experience for the guest. (NEUHOFER, B.et al., 2015).

1.2.6. Wearable devices

Wearable devices, above listed as vi., are body-attached computers and a part of the *IoT,* therefore contributing to ubiquitous computing. Currently, there are different types of wearables applied to tourism destinations: 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; and 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; so, visitors can easily switch between real objects and augmented reality (ATEMBE, R., 2015).

All these wearables have in common the fact that they collect and process user-specific data. Alongside body-data, many of them 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 another challenge for data protection and privacy. Moreover, the use of wearable devices does not only involve its user (in general, 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 (JÜLICHER, T.; DELISLE, M., 2018).

1.2.7. Big data analytics

Tourism data is an asset being exploited using a multi-modal pipeline of advanced data analysis methods called big data analytics (WATERMAN, K.; BRUENING, P., 2014). These, comprise content analytics crawlers (mining unstructured content), machine learning (ML) algorithms, natural language processing tools (NLP) and data mining techniques (DM). Distinctive aspects of big data analytics trigger implications on data protection, for example: i. Use of large numbers of ML algorithms against data to find correlations, inferences between data. ii. Once relevant correlations are identified (even if 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 (MANTELERO, A.; VACIAGO, G., 2013).

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 (EDWARS, L., 2016), with the aim of achieving more satisfaction (LAW, Rob *et al*., 2009)at the experience environment.

1.3. Sources and types of tourism data

As we have just seen, tourism-related data has multiplied geometrically (MANYIKA, J. *et al*., 2011) through its heterogeneous provenance (SNSs, apps, sensors, etc., as observed in the former section). Thisdata sources provide a massive size of volunteered, observed, inferred or collected digital traces, resulting in multidimensional sets of data, known as big data (HABEGGER, B. *et al*., 2014). So, the 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, comprises, for example: i. transactional data, exchanged between tourists and transportation and hospitality undertakings (airlines, hotel, restaurants and rental car businesses) derived from queries/searches, purchases, and other exchanges; ii. geographical data, such as GPS position; iii .temporal data; vi. UGC and opinion data derived from client's profiles, established preferences, needs, opinions, etc.; v. Textual tourism data on the web, consisting in rich *corpora* for linguistic analysis.

Such heterogeneity of data holds strategic commercial value. As a matter of fact, it can expose the commercial preferences of its users, allows the detection and prediction of future behaviors and trends, rendering huge interest for both public and private sectors. Besides, allows destinations to better plan for future tourists in terms of mobility, popular attractions, tailored package holidays, and other potential issues. By managing such big data, tourism organizations can extract value from information that may take them to a new dimension of customer experience and improve the way they interact with tourists, hence gaining competitive advantages (BUHALIS, D.; AMARANGGANA, A., 2014). Such information is the fabric for companies to turn big and *open data* into future preferences and value propositions (PANTANO, E., *et al.*, 2017).

Even though the identified 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 incorporate the risk of building a detailed profiles of tourists, actually, a holistic personal mosaic of each individual user, with imminent risks for privacy and data protection (DAVENPORT, Th. H., 2013; RUBINSTEIN, I.S., 2013; KEMP, R., 2014; and, MASSENO, M.D., 2016).

2. **Risks ofSmart Tourism Destinations to Privacy and Data Protection and Compliance towards the GDPR**

In this section we try to explain some of the potential risks STD technologie sent ail to privacy and data protection. Besides, we'll summon the compliance tools that can help STD organizations meet their data protection obligations and protect people's privacy rights in a STD context, and they are: anonymization and pseudonymization, privacy policies, data protection impact assessment, privacy by design, personal data stores, algorithmic transparency and privacy seals/certification.

2.1. Risks Inherent to a Huge Digital Footprint

Is well known that the use and combination of advanced techniques of*big data analytics*, which includemachine learning (ML), data mining techniques (DM), etc., enhance the common risks hampering privacy and data protection (DAVENPORT, Th.H., 2013).The following are enhanced when information (e.g. mobility data) is connected and matched with data from other sources of publicly available information (e.g.*Facebook* or *Twitter* postings, blogs entries, etc.) and analysis revealed users' social interactions and activities (ANUAR, F.I.; GRETZEL, U., 2011), as forsmart tourist travel cards (ROMANOU, A., 2018).

2.1.1. Identification and re-identificationofindividualsfrom allegedly anoymised or pseudonymised data.

These concerns rely on the fact that integrating large collections of data from distinct sources of available tourism datasets, even with apparently innocuous, non-obvious or anonymized resources, may enhance a jigsaw of indirect correlation of identification and re-identification; this scenario could escalate if massive information resources via the web is available (Art. 29 WP Opinion 7/2003; Opinion 3/2013; and Opinion 6/2013). Thereby, personal information set through re-identification intrinsically abides to legal requirements, as identification not only means the possibility of retrieving a person's name and/or address, but also includes potential identifiability by singling out, *linkability* and inference (Art. 29 WP Opinion 05/2014; and, LEONARD, P., 2014).As data collected by the ubiquitous computing sensors is, in principle, personal data(Art. 29 WP Opinion 4/2007) or "personally–identifiable information", the processing of non-sensitive data can lead, through data mining, to data that reveals personal or sensitive information, thus, blurring the conventional categories of data.

2.1.2. Covert profiling of individuals and non-transparency of the processing

Profiling is an important feature in tourism destinations. Tourism service providers are adapting their serviceable approach to meet the personalization expectation of costumers. 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 designed to extract as much surplus from the user as possible (ENISA 2015 Report). 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." (Art. 29 WP Opinion 8/2014).However, the GDPR prohibits automated individual decision-making that significantly affect individuals, Art. 22 (1).

Indeed, developments on consumer-tourist automated profiles, facilitated by big data analytics, can *significantly affect* data subjects (EDPS Opinion 3/2015). 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 (PARISER, E., 2011), 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.

Besides, 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 (SCHWARTZ, P.; SOLOVE, D., 2011). In this synopsis, tourists might be discriminated against as they belong to a social group, but also such ascertainment might be based on factors, identified by the analytics, that they share with members of that group. Therefore, to ensure a fair and transparent processing (as set by the principle of fairness and transparency), automated decisions should account all the circumstances concerning the data and not be based on merely de-contextualized information or on data processing results. Moreover, the data 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 of GDPR.

2.1.3. Repurposing of data

As data analytics can mine data for new insights and find correlations between apparently disparate datasets; hence, automatic capture of big data can be mostly reused (Art. 29 WP Opinion 03/2013) for secondary unauthorized purposes, profiling, or for abusive marketing activities, undermining the purpose specification principle convening that the purpose for which the data is collected must be specified andlawful, Art. 5(1) (b). As for a repurpose, personal data should not be further processed in a way that the datasubject might consider unexpected, inappropriate or otherwise objectionable (COE Guidelines) and, therefore, unconnected to the delivery of the service.

2.1.4. Surveillance under the disguise of service provision and its desensitizing effect.

Data subject's interactions in a smart destination environment will be increasingly mediated by or delegated to (smart) devices and apps. Most of the destinations are using video-surveillance systems as sensors to supply real-time information on public transportation, traffic, in the domains of emergency and personal safety, navigation, and access to tourist information on the go, which all provide value to the user: safety, convenience, and utility indaily lives, as well as in vacation. Such information is transmitted via, for e.g.,smart remote controllable digital CCTV cameras that can zoom, move and track individual pedestrians, ANPR (number plate) recognition, GPS,Wi-Fi network tracking reliable facial recognition software, location-based service apps (LBS) (NEUHOFER, Barbara *et al*., 2015). It has been argued that such devices desensitize users about providing location-based information because of the ease with which it happens and the "coolness" factor that comes with it(SARAVANAN, Sh.; SADHU RAMAKRISHNAN, B., 2016).

2.1.5. Failed consent

In this sort of intelligent environments, it is problematic to give, or withhold, our prior consent to data collection (KITCHIN, R., 2016), as it seems to be absent by design. The absence of 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 may, 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 also perceive 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. So, the main 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 (SCHWARTZ, P.; SOLOVE, D., 2011) and thereupon, users do not hold the opportunity give their unambiguous, informed, specific, explicit, and granular consent (Art. 29 WP Opinion 15/2011; Art. 29 WP Guidelines; and, MANTELERO, A., 2014). Therefore, the data controller might have difficulty in demonstrating that the consent was given, and the data subject is not able to withdraw that consent (CAROLAN, E., 2016).

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) (Art. 29 WP Opinion 8/2014).

2.1.6. Imbalance

Smart technologies 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 consequence of enhanced information asymmetry (MASSENO, M.D., 2016).

2.1.7. Tendency to collect and analyze all data

The tourism industry is inherently based on data-exchange: to generate massive databases, is necessary to optimally exploit all information available and as so, datasets need to be exhaustive and varied as possible to faithfully reflect the touristic activity of a territory (SOUALAH-ALILA, F. *et al.*, 2016).In substance, smart technology purports the extensive collection, aggregation and algorithmic analysis of all the available data for various reasons, such as understanding customer buying behaviours and patterns or remarketing based on intelligent analytics, hampering the data minimization principle (Art. 5 (1) (c). In addition, irrelevant data is being also being collected and archived, undermining the storage limitation principle(Art. 5 (1) (e).

2.1.8. Inaccurate data

Results drawn from data analysis may not be representative or accurate, 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). Machine learning itself may contain hidden bias which lead to inaccurate predictions and profiles about individuals. Profiling involve creating derived or inferred data, occasionally leading to incorrect decisions (discriminatory, erroneous and unjustified, regarding their behaviour, health, creditworthiness, recruitment, insurance risk, etc.) (EDWARDS, L., 2016). Even exercising the "*right to be forgotten*", 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 thepurpose for which it was collected, or based on inaccurate data (as set by the accuracy principle depicted inArt. 5 (1) (d). In fact, it may be difficult for a business to find and erase someone's data if it is stored across several different systemsand jurisdictions (BARTOLINI, C.; SIRY, L., 2016).

2.2. **Compliance toolsat the GDPR**

At this point, we should underline thatcurrent access and reuse of tourism information within the framework of a STDcollides with the legal standards for which the GDPR was designed.However, compliance tools may 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.

2.2.1. **Anonymization**

In principle, when data is rendered *anonymous* (Recital 26 of the GDPR) all identifying elements have been irreversibly eliminated from a set of personal data, and cannot leave space to re-identify the person(s) concerned; therefore, it is deemed to be no longer personal data. Later, anonymised data might be aggregated to be analysed and to gain insights about the population as a whole, as well ascombined with data from any other sources. At this stage, *IoT* developers can analyse, share, sell or publish the data without data protection requirements.

Conversely, de-anonymization strategies in DM entails that anonymous data is cross-referenced with other sources to re-identify the anonymous data. Thus, the processing of datasets rendered anonymous may never be absolutely ensured(OHM, P., 2010).

In what refers to *pseudonymized* personal data, identifiers are replaced by a pseudonym (through encryption of the identifiers). In turn, pseudonymized data continues to allow an individual data subject to be singled out and linkable across different datasets and therefore stays inside the scope of the legal regime of data protection (Art. 29 WP Opinion 05/2014).

2.2.2. **Privacy policies**

Now a core issue, these consist of multiple paragraphs of natural language disclosing an organization's data practices on processing activities of personal data to its users, such as collection, use, sharing, and retention. They serve as a basis for decision-making, a "tool for preference-matching" for consumers, as consumers value a product/service more, after learning more about its attributes and tradeoffs for making a consumption decision. As such, they constitute the locus1 where consequences are produced, the "technically most feasible place to protect privacy and personal data (SANTOS, C. *et al*., 2017).

The GDPR states that information addressed to the data subject should be "concise, easily accessible and easy to understand, and that clear and plain language, and additionally, where appropriate, visualisation is used", Article 12(7) and Recital 60. However, in a smart tourism destination scenario, these requirements can be problematic, and it has been suggested that privacy notices are not feasible when big data analytics perform, by reason of: travelers engaged in tourism experiences are unwilling to read lengthy legalese privacy notices, since it would take significantly more time than they spend using the content or the app; the context in which data is collected (e.g., destination apps, wearable watches and glasses or IoT devices) is difficult to provide the information. 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 (HABEGGER, B. *et al*., 2014).On the other hand, information can be delivered in a user-friendly form, namelyby videos or in-app notices; cartoons and standard icons applied to privacy notices, explaining their content; as for wearable devices, privacy information could be provided on the device itself, or by broadcasting the information via Wi-Fi or making it available through a QR code (Art. 29 WP Opinion 8/2014)

2.2.3. Data protection impact assessment

A data protection impact assessment (DPIA) is a tool that can help to identify and mitigate privacy risks, before the processing of personal data. This assessment involvesa description of the envisaged processing operations, an evaluation of the privacy risks and the measures envisaged to address those risks. Art. 35 of GDPR denotes that when a type of processing resorting to a systematic and extensive evaluation of individuals based on automated processing and profiling, significantly affecting individuals using new technologies, and when such a processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged operations on the protection of personal data. So, it is most likely that general big data applications involving the processing of personal data, within a STD, will fall into this category.

2.2.4. Privacy by design

By design solutions (PbD) consist in an approach in which IT system designers should code preemptive technological and organizational measures when conceiving specifications and their architecture, early at the development stage of new products and services. It aims to address privacy concerns applied to the very same technology that might create risks (Art. 25) (ZUIDERVEEN BORGESIUS, F.J., 2016). Besides anonymization techniques, PbD involves other engineering and organizational measures, including: security measures such as access controls, audit logs and encryption; data minimization measures, to ensure that only the personal data that is needed for a particular analysis or transaction is processed at each step (such as validating a customer);purpose limitation and data segregation measures so that, for example, personal data is kept separately from data used for processing intended to detect general trends and correlations (SOLOVE, D., 2017); and, sticky policies' that record individual's preferences and corporate rules within the metadata that accompanies data (LEONARD, P., 2014).

At a STD scenario, controllers and processors should test the adequacy of the above-mentioned solutions by-design on a limited amount of data by means of simulations before their use on larger scales, in a learn-from-experience approach. This would make it possible to assess the potential bias of the use of different parameters in analyzing data and provide evidence to minimize the use of information. However, there is a lack of a privacy mindset in IT system designers (HADAR, I. *et al*., 2018), also stated by ENISA

> [...]privacy and data protection features are, on the whole, ignored by traditional engineering approaches when implementing the desired functionality. This ignorance is caused and supported by limitations of awareness and understanding of developers and data controllers as well as lacking tools to realise privacy by design. While the research community is very active and growing, and constantly improving existing and contributing further building blocks, it is only loosely interlinked with practice.(ENISA 2015 Report).

2.2.5. **Personal data spaces**

The European Data Protection Supervisor suggested that one way to increase an individual's control over the use of their data is through what are usually called personal data spaces, vaults or stores (EDPS Opinion 7/215), or also denominated by personal information management services. These are third-party services (intermediaries) that collect, manage and store people's personal data on their behalf and make it available to organisations as and when the individuals wish to do so (ABITEBOUL, S. *et al*., 2015).This tool aims to address the critics related to the lack of control of how personal data is used in a big data environment, as tourists are not aware of how data is being collected or how it is used, and don't have the time to read privacy notices.

2.2.6. **Algorithmic transparency**

Namely, the following suggestions on the view of algorithmic transparency are reflected in the findings of research of the Information Commissioner´s Office of the UK (ICO Guide 2017): Techniques for algorithmic auditing can be used to identify the factors and make transparent the algorithm step-by-step development that influence an algorithmic decision and assure public trust;Interactive visualization systems can help individuals to understand why a recommendation was made and give them control over future recommendations; and, Ethics board scan be used to help shape and improve the transparency of the development of machine learning algorithms.

2.2.7. Privacy seals and certification

Certification schemes (Arts. 42, 43, Recital 100) can be used to help demonstrating data protection compliance of STD big data processing operations. They encourage the "establishment of data protection certification mechanisms and of data protection seals and marks" to demonstrate that processing operations comply with the Regulation. These would be awarded by data protection authorities or by accredited certification bodies (RODRIGUES, R., 2016; and, ENISA 2017 Recommendations).

Conclusions

The preceding analysis brings out thatsmart tourism is becoming a big contributor and benefactor of ubiquitous, always-on data capture about customers towards enhanced tourism experiences, and competitive markets. This extensive collection and processing of personal data in the context of STD 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. The apprehension here is to understand if the affordances of the technology, the personalized services, and enhanced experiencescan cope with data protection obligations without such a micro-targeting and profiling. As we have seen, Smart Tourism raises big issues with respect to information governanceand about correctly deriving the "added" value from information in an open and ubiquitous info-structure. As for now, the current assumption is that all captured information is extremely valuable and necessary to organizations and will be freely provided by tourists who seek enriched tourism experiences(TALLON, P., 2013). Moreover, the lack of privacy and data protection mindset of engineers and coders working in *IoT/Cloud* businesses poses a very large problem for the future (SCHWARTZ, P.; SOLOVE, D., 2011). It is suggested that STDare to proceed with test prototyping and research before the implementation of new technologies andservices in large-scale real-life environments, such asthe *Mobile Living Lab* (EDWARDS, L., 2016). Finally, besides addressing related information security issues according to the *NIS Directive*, (Directive (EU)

2016/1148), future research regarding mobile devices and tracking will be needed, moreover following the adoption of the future e *Privacy Regulation* (EU Proposal for a Regulation - COM/2017/010 final).

References

-ABITEBOUL, Serge *at al*. **Managing your digital life with a Personal information management system**.Communications of the ACM, ACM, 2015, 58 (5), pp.32-35, accessible at https://hal.inria.fr/hal-01068006/file/pims.pdf, consulted on 20/05/2018.

- ANUAR, Faiz I.; GRETZEL, Ulrike. **Privacy Concerns in the Context of Location-Based Services for Tourism**.ENTER 2011 Conference. Accessibility of ICTs and Accessible Travel Information, Innsbruck, Austria, 2001,accessible at http://agrilifecdn.tamu.edu/ertr/files/2013/02/13.pdf, consulted on 20/05/2018.

ART 29 WP – Article 29 Work Party of the European Union. **Opinion 7/2003**, on the re-use of public sector information, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf, consulted on 20/05/2018.

_______. **Opinion 4/2007**, on the concept of personal data, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, consulted on 20/05/2018.

_______. **Opinion 15/2011**, on the definition of consent, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, consulted on 20/05/2018.

_______. **Opinion 3/2013**, on purpose limitation, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, consulted on 20/05/2018.

_______. **Opinion 6/2013**, on open data and public-sector information (PSI) reuse, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf, consulted on 20/05/2018.

_______. **Opinion 05/2014**, on anonymisationtechniques, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, consulted on 20/05/2018.

_______. **Opinion 8/2014**, on the recent developments on the Internet of Things, accessible at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, consulted on 20/05/2018.

______. **Guidelines on Consent under Regulation 2016/679**, accessible at http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030, consulted on 20/05/2018.

- ATEMBE, Roland.**The Use of Smart Technology in Tourism: Evidence from Wearable Devices**. *Journal of Tourism and Hospitality Management*, Amsterdam, Vol. 3, n. 11-12, 2015, pp. 224-234.

- BARTOLINI, Cesare; SIRY, Lawrence. **The right to be forgotten in the light of the consent of the data subject**. Computer Law and Security Review, Amsterdam, Vol. 32, n. 2, 2016, pp. 218-237.

- BAUZÀ M., Felio. **Tourism, Technology and Citizens' Legal Protection: Tourism Data**. Athens Journal of Tourism, Athens, Vol. 5, n. 1, 2018, pp. 55-68.

- BUHALIS, Dimitrios. **Marketing the Competitive Destination of the Future**. Tourism Management,Amsterdam, Vol. 21, 2000, pp. 97–116.

- BUHALIS, Dimitrios; AMARANGGANA, Aditya. **Smart Tourism Destinations**.In XIANG, Zheng; TUSSYADIAH, Lis (Eds.).Information and Communication Technologies in Tourism 2014 - Proceedings of the International Conference in Dublin, Ireland. Heidelberg: Springer, 2014, pp. 553-564.

- BUHALIS, Dimitrios; AMARANGANNA, Aditya. **STD: Enhancing Tourism Experience Through Personalisation of Services**. In TUSSYADIAH, Lis; INVERSINI, Alessandro (Eds.).Information and Communication Technologies in Tourism 2015 - Proceedings of the International Conference in Lugano, Switzerland. Heidelberg: Springer, 2015, pp. 377-389.

- CAROLAN, Eoin. **The continuing problems with online consent under the EU's emerging data protection principles**. Computer Law and Security Review, Amsterdam, Vol. 32, n. 3, 2016, pp. 462-473

- ČAS, Johann.**Ubiquitous Computing, Privacy and Data Protection**.In GUTWIRTH, Serge *et al.* (Eds.). Computers, Privacy and Data Protection: An Element of Choice. Heidelberg: Springer, 2009, pp. 139-169.

- COE – Council of Europe. **Guidelines** on the Protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD, 2017, accessible at https://rm.coe.int/16806ebe7a, consulted on 20/05/2018.

- DAVENPORT, Thomas H. **At the Big Data Crossroads: turning towards a smarter travel experience**. Amadeus IT Group Report, 2013, accessible athttp://www.amadeus.com/web/binaries/blobs/703/769/Amadeus_Big_Data,1.pdf, consulted on 20/05/2018.

- EDPS – European Data Protection Supervisor. **Opinion 3/2015**, Europe's big opportunity, EDPS Recommendations on the EU's options for data protection reform, accessible at https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf, consulted on 20/05/2018.

-_______. **Opinion 7/2015** on Meeting the challenges of big data, accessible at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf, consulted on 20/05/2018.

- EDWARDS, Lilian. **Privacy, security and data protection in smart cities: a critical EU law perspective**. European Data Protection Law Review, Berlin, Vol. 2, 2016, pp. 28-58.

- ENISA – European Networks and Information Security Agency. **2015 Report** on *Privacy and Data Protection by Design – from policy to engineering*, accessible at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport, consulted on 20/05/2018.

_______. **2017Recommendations** on European Data Protection Certification, accessible at https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport, consulted on 20/05/2018.

- EU – European Union. **Regulation (EU) 2016/679**, of the European Parliament and of the Council of 27/04/2016, 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 of 2018, accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, consulted on 20/05/2018.

_______.**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, accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, consulted on 20/05/2018.

_______.**Proposal for a Regulation** of the European Parliament 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), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN, consulted on 20/05/2018.

- GRETZEL, Ulrike; SIGALA, Marianna *et al.* **Smart tourism: foundations and developments**. Electronic Markets, Heidelberg, Vol. 25, n. 3, 2015, pp. 179–188.

- GRETZEL, Ulrike; REINO, Sofiaet *al.* **Smart Tourism Challenges**. Journal of Tourism, Garhwal University,Vol. 16, n. 1,2015, pp. 41-47.

- ICO - Information Commissioner's Office. **Guide** on Big Data, Artificial Intelligence, Machine Learning and Data Protection, 2017, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/, consulted on 20/05/2018.

- HABEGGER, Benjaminet *al.* **Personalization vs. Privacy in Big Data Analysis**. International Journal of Big Data. New York, n. 1, 2014, pp. 25-35.

- HADAR, Iritet *al.* **Privacy by designers: software developers' privacy mindset**. Empirical Software Engineering.Heidelberg, Vol. 23, n. 1, 2018, pp 259–289.

- HOEREN, Thomas. **Big Data and Data Quality**.In HOEREN, Thomas; KOLANY-RAISER, Barbara (Eds.), Big Data in Context - Legal, Social and Technological Insights. Heidelberg: Springer, 2018, pp. 1-11.

- HÖJER, Mattias; WANGEL, Josefin, **Smart Sustainable Cities: Definition and Challenges**. In HILTY, Lorenz; AEBISCHER, Bernard (Eds.). ICT Innovations for Sustainability, Advances in Intelligent Systems and Computing. Heidelberg: Springer, 2015, pp. 333-349.

- JÜLICHER, Tim; DELISLE, Marc. **Step into 'The Circle'—A Close Look at Wearables and Quantified Self**. In HOEREN, Thomas; KOLANY-RAISER, Barbara (Eds.). *Big Data in Context - Legal, Social and Technological Insights*, Heidelberg: Springer, 2018, pp. 81-91.

- KEMP, Richard. **Legal aspects of managing big data**. Computer Law and Security Review, Amsterdam, Vol. 30, n. 5, 2014, pp. 482-491.

- KITCHIN, Rob. **Getting smarter about smart cities: Improving data privacy and data security**. Dublin: Data Protection Unit / Department of the Taoiseach, 2016, accessible athttp://eprints.maynoothuniversity.ie/7242/, consulted on 20/05/2018.

- LAW, Rob *et al*. **Information technology applications in hospitality and tourism: a review of publications from 2005 to 2007**. Journal of Travel & Tourism Marketing, Abingdon-on-Thames, Vol. 26, n. 5-6, 2009, pp. 599-623.

- LEONARD, Peter. **Customer data analytics: privacy settings for 'Big Data' business**. International Data Privacy Law, Oxford, Vol. 4, n. 1, 2014, pp. 53-68.

- LUZAK, Joasia, **Vulnerable Travellers in the Digital Age**. Journal of European Consumer and Market Law, München, Vol. 5, n. 3, 2016, pp. 130-135.

- MANTELERO, Alessandro. **The future of consumer data protection in the E.U. Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics**. Computer Law and Security Review, Amsterdam, Vol 30, n. 6, 2014, pp. 643-660

-_______. **Data protection, e-ticketing, and intelligent systems for public transport**.International Data Privacy Law, Oxford, Vol 5, n. 4, 2015, pp. 309-320.

- MANTELERO, Alessandro; VACIAGO, Giuseppe. **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. Computer Law Review International, Berlin, Vol. 14, 2013, pp. 161-169.

- MANYIKA, James *et al*. **Big data: The next frontier for innovation, competition, and productivity**. Report - McKinsey Global Institute, 2011,accessible athttps://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation, consulted on 20/05/2018.

- MASSENO, Manuel David. **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**. Comparazione e diritto civile.Salerno, n. 4, 2016, 1-14.

- NEUHOFER, Barbara *et al.* **Smart technologies for personalized experiences: a case study in the hospitality domain**. Electronic Markets, Heidelberg,Vol 25, n. 3, 2015, pp. 243-254.

- OHM, Paul. **Broken promises of privacy: Responding to the surprising failure of anonymization**. UCLA LawReview, Los Angeles, Vol. 57, n. 6, pp. 1701-1777, 2010.

- PANTANO, Eleonora *et al.* **'You will like it!' Using open data to predict tourists' responses to a tourist attraction**.Tourism Management, Amsterdam, Vol. 60, 2017, pp. 430-438.

- PARISER, Eli.**The Filter Bubble: What the Internet is Hiding from You**. New York: The Penguin Press, 2011.

- PIHLSTRÖM, Minna, *Perceived Value of Mobile Service Use and its Consequences*. Helsinki: Swedish School of Economics and Business Administration, 2008, accessible athttps://helda.helsinki.fi/bitstream/handle/10227/269/176-978-951-555-977-7.pdf?sequence=2&origin=publication_detail, consulted on 20/05/2018.

- PRAHALAND, C. K.; RAMASWAMY, Venkat. **Co-creation experiences: the next practice in value creation**. Journal of Interactive Marketing, Amsterdam, Vol. 18, n. 3, 2004, pp. 5-14.

- RODRIGUES, Rowena *et al.* **The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR**. International Review of Law, Computers & Technology, Abingdon-on-Thames, Vol. 30, n. 3, 2016, pp. 248-270.

- ROMANOU, Anna. **The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise**. Computer Law and Security Review, Amsterdam, Vol. 34, n. 1, pp. 99-110

- RUBINSTEIN, Ira S. **Big Data: The End of Privacy or a New Beginning**. International Data Privacy Law, Oxford, Vol. 3, n. 2, 2013, pp. 74-87.

- SANTOS, Cristiana *et al.* **Detecting and Editing Privacy Policy Pitfalls on the Web**. In Proceedings of 1st Workshop on Technologies for Regulatory Compliance / 30th International Conference on Legal Knowledge and Information Systems (JURIX).University of Luxembourg. Luxembourg, 13th of December 2017, pp. 87-99,accessible athttp://ceur-ws.org/Vol-2049/09paper.pdf, consulted on 20/05/2018.

- SARAVANAN, Shanti; SADHU RAMAKRISHNAN, Balasundaram. **Preserving privacy in the context of location based services through location hider in mobile-tourism**. Information Technology & Tourism, Heidelberg, Vol. 16, n. 2, 2016, pp 229–248.

-SCHWARTZ, Paul; SOLOVE, Daniel.**The PII Problem: Privacy and a New Concept of Personally Identifiable Information**.New York University Law Review, Vol. 86, 2011, pp. 1814-1894.

- SOLOVE, Daniel. **I've Got Nothing to Hide and Other Misunderstandings of Privacy**. San Diego Law Review, San Diego, Vol. 44, 2017, pp. 745–772.

- SOUALAH-ALILA, Fayrouzet *al*. **DataTourism: Designing Architecture to Process Tourism Data**. In INVERSINI, Alessandro; SCHEGG, Roland (Eds.), Information and Communication Technologies in Tourism 2016 - Proceedings of the International Conference inBilbao, Spain. Heidelberg: Springer, 2016, pp. 751-763.

- TALLON, Paul. **Corporate governance of big data: perspectives on value, risk, and cost**. Computer, Long Beach, Vol. 46, Issue 6, 2013, pp. 32-38.

- TUSSYADIAH, Lis; FESENMAIER, Daniel. **Mediating the tourist experiences access to places via shared videos**. Annals of Tourism Research, Amsterdam, Vol. 36, n. 1, 2009, pp. 24-40.

- WATERMAN, K.; BRUENING, Paula, **Big Data analytics: risks and responsibilities**. International Data Privacy Law, Oxford, Vol. 4, n. 2, 2014, pp. 89-95.

- ZUIDERVEEN BORGESIUS, Frederik J. **Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation**. Computer Law and Security Review, Amsterdam, Vol. 32, n. 2, 2016, pp. 256-271.