Intelligent Environments 2018
I. Chatzigiannakis et al. (Eds.)

doi:10.3233/978-1-61499-874-7-298

Privacy and Data Protection Issues on Smart Tourism Destinations – A First Approach[1]

Manuel David MASSENO[2,a], Cristiana SANTOS[b]
[a]*LabUbiNET, Instituto Politécnico de Beja, Portugal*
[b] *DH-CII, Universidade do Minho, Portugal*

Abstract. Data lies at the core of all smart tourism activities as tourists engage in different and personalized touristic services while traveling 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 Smart Tourist Destinations to create enriched, high-value tourism experiences for tourists, as well as granting destinations with competitive advantages. The perceived enjoyment has to be considered within the legal framework of data protection by exposing potential risks to data protection and privacy, as well as the available answers given by the General Data Protection Regulation.

Keywords. Privacy and Data Protection, Smart Tourism Destinations

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, being this paper a sort of primer endeavor[3]. 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 enhance the competitiveness of each destination.

[1] Paper drafted within the framework of the Research Project: "*Big Data*, *Cloud Computing* y otros retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico" - DER2015- 63595 (MINECO/FEDER), Coordinated by Professor Apollònia Martínez Nadal at the *Universitat de les Illes Balears*, Spain.

[2] Corresponding author: mdmasseno@gmail.com

[3] 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.

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 costumers loyalty, much harder [10]. 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 [10], suggesting that personal data and privacy concerns might be temporarily 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 [20]. 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. The following illustrative examples provide insight towards possible 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 particular direction to get on, and also 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, in order 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 [8]. So, it is argued that privacy and data protection research is needed in the Tourism context, balancing the tradeoff 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 briefly its origin, constituents, added-value and objectives. Section 2 provides some of the most important risks that can be appointed to STD regarding privacy and data protection, and its corresponding compliance to the General Data Protection Regulation[4], 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 describes the constituents of STD, objectives and derived added value.

[4] Regulation (EU) 2016/679, of the EP 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.

1.1. *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 structured into six axes or "6As" as the literature describes [7], 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 then additionally 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"*[4]. This embracing concept comprises three core elements [6]:

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 [5]. IoT could support in terms of providing information and analysis as well as automation and control. For instance, chips embedded to entrance ticket, or a smartphone app, allow tourism service providers to track tourists' locations and their consumption behavior, enabling location-based advertising. 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. A Smart Destination is conceived as "*an innovative tourist destination, built on an infrastructure of state-of-the-art technology guaranteeing the sustainable development of tourist areas, 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"* [6]; and

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

1.2. *Smart Tourism Experiences*

The shared *purpose* of all omni-channel stakeholders of a smart tourism ecosystem is the availability of enhanced/enriched, high-value, meaningful and sustainable tourism experiences through smart services and products [7]. Therefore, and at least potentially, STD enhance tourism experience through the offer of products/services that might be customized in order to meet each of visitor's unique needs and even implied desires, as for understanding the needs, wishes and desires of travelers becomes increasingly critical for the attractiveness of destinations. Hence, tourism data has multiplied, geometrically [3]. This data is being conveyed through several sources: i.online social networks; ii. online reviews/ratings; iii. intelligent location sensors in interaction with mobile devices; iv. transactional communications based on reservations by transportation/hospitality undertaking (airlines, hotel, restaurants and rental car businesses, namely)[5]. Each of these sources provide a massive size of digital traces (data trails or digital footprint), resulting in multidimensional sets of data, known as Big Data [14]. This massification of real-time (tourism) data, from different sources, 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. Besides, tourism data reveals specific features, as it holds strategic value, allowing the detection and prediction of future behaviors and trends, allows for the analysis of development and optimization processes of products/services, retention of customers, and ultimately is useful for future decision-making. This flow of data, inherently cross-border, may consist in personal data, geographical, transactional data (derived from queries/searches, purchases, and other exchanges), feedback data, respectively. These data can reveal commercial preferences of its users, rendering enormous interest for economic operators, and allow cities to better plan for future tourists in terms of mobility, popular attractions, and other potential issues. By managing 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 [8]. As STD experiences are achieved through intensive personalization, context-awareness and real-time monitoring [8], [9], this entails legal risks, demanding a careful analysis within data protection framework (as approached in the following section).

2. Risks of Smart Tourism Destinations to Privacy and Data Protection

In this section we explain concerns that STD technologies entail to privacy and data protection.

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 include machine learning (ML), data mining techniques (DM), content analytics crawlers (mining unstructured content), potentiate known risks hampering privacy and data protection [22]. As deployed algorithms reach beyond usual analytics, leading to the finding of inferences, connections and relationships between data even for neither originally unforeseen nor previously unknown onuser pictures, real names and can also often be used as unique or near unique identifiers across multiple databases. Based on these correlations, predictions will be made, and a new algorithm can be created and applied to particular cases in the future. The following risks are fueled when information (e.g. mobility data) is conjoined and matched with data from other sources of publicly available information (e.g. Facebook or Twitter postings,

[5] 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.

blogs entries, etc.) and analysis revealed users' social interactions and activities, as occurred with public bike data[6] or smart tourist travel cards [25].

a. Identification and re-identification[7] *of individuals from allegedly anonymised or pseudonymised data.* Alleged concerns relies 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 there is access to rich information resources via the web. 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 [23] [8].Data collected by the ubiquitous computing sensors, are, in principle, personal data[9] or "personally–identifiable information"[11], as 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.In principle, when data is rendered *anonymized* (recital 26, 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 and IoT developers are be able to release, sell or publish the data without data protection requirements. Conversely, de-anonymization strategy in data mining 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 ensured. When personal information is *pseudonymized*, 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[10].

b. Profiling of individuals. The integration and matching techniques of tourism datasetsknowledge can be produced about users and hence the creation of profiles: consumer, movement, or social profiles. Profiling vests companies, public authorities to determine, analyse or predict people's personality, behaviour, and preferences without their cognition, and make also possible to refer these behaviours and attitudes to perfectly identified individuals. Such processes may and are likely to epitomize privacy invasiveness or even waiving the data subjects' control upon their data. The GDPR prohibits automated individual decision-making that significantly affect individuals (Arts. 22(1) and 4(4)), such as profiling. However, secret-tracking and decision-making on the basis of profiles are hidden from any individual, which is left without meaningful information about the "algorithmic logic" which develops these

[6] See, J Siddle, "I Know Where You Were Last Summer: London's Public Bike Data Is Telling Everyone Where You've Been" (2014),http://vartree.blogspot.co.uk/2014/04/i-know-where-youwere-last-summer.htm

[7] See Art. 29 WP Opinion 6/2003 on the Re-use of public sector information, Opinion 3/2013 on Purpose Limitation", and Opinion 6/2013 on Open Data and Public Sector Information (PSI) reuse.

[8] EDPS Opinion 05/2014 on Anonymisation Techniques, p. 10

[9] Art. 29 WP Opinion 4/2007 on the Concept of Personal Data.

[10] EDPS Opinion 05/2014 on Anonymisation Techniques, p. 10.

profiles and has an effect on the data subject[11]. In fact, "(…) *analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behaviour patterns.[12]*" Likewise, in a STD, this can lead to an exclusion/denial of services/goods, e.g. denial of insurances, exclusion from the sale of certain touristic or high-end products, shops or entertainment complexes, even essential utilities for those unwilling to share personal data [12]. Tourism service providers are adapting their serviceable approach to meet the "personalization" expectation [13]. Personalization is attained by collecting and utilizing personal information about needs/preferences (facilitated in a STD scenario), to be able to provide offers and information fitting perfectly clients' needs. Therefore, user's input and feedback are used to build profiles and recommender systems in the form of trail packages, which for some can be considered a risk of "data determinism", in which individuals are not merely profiled and judged on the basis of what they have done, but also a prediction of what they might do in the future[14].

c. *Repurposing of big data*. Automatic capture of big data through sensors is collected for secondary unauthorized purposes, or for abusive marketing activity, this way, undermining the purpose specification and use limitation principles.

d. Surveillance under the disguise of service provision and 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 in daily 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)[10]. 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. These developments require devising specially protected digital spaces for children which are particularly vulnerable in the face of data processing practices.

e. *Failed consent.* In this intelligent environment, it is dubious to give or withhold our prior consent to data collection [15], 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. The issue of the IoT, also within a STD, is that its sensorization devices are explicitly designed to be unobtrusive and seamless, invisible in use and unperceived to users[12] and thereupon, users do not hold the opportunity give their

[11] EDPS, Opinion 3/2015, p. 8

[12] Art. 29 WP Opinion 8/2014 on the on Recent Developments on the Internet of Things

unambiguous, informed, specific (intelligible that specifies the exact purpose of the processing), explicit, and granular consent[13]. However, 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)[14]. 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 [14]. Reverting 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". As most commercial systems rely on the "legitimate interests" ground, even if they are "the vaguest ground for processing[15], and offers a lot of scope for industry to process data if they can claim a "legitimate interest", delegation of the task of balancing commercial interests and user fundamental rights to the controller themselves [12].

f. 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 [2].

2.2. *Compliance to the GDPR*

At this point, we should underline that access and reuse of information within the framework of a STD collides with legal standards for which the GDPR was designed. So, we will now bestow attention to the following fundamental principles, which all organizations must follow whilst processing personal data related to any STD environment.

a. *Lawfulness, Fairness and Transparency.* For a first, these principles require that when the data is collected, it must be clear as to why that data is being collected and how the data will be used (Art. 5, clause 1(a)). Even so, big data algorithms producing results are usually invisible and opaque to the user, and its results often impenetrable to laymen; algorithms can learn and change in a semi-autonomous way, making them hard to document, also due to their copyright protecting the software and trade-secret shield [12]. We are attentive to a right to know the "*logic of the processing*" applied to our data (Recital 63, and Arts. 13(2) (f), and 15(1) (h), respectively).

b. Purpose Limitation (Art. 5(1) (b) Big Data analytics, inherent to STD, often engage in processing data for purposes that had not been initially scheduled, or still to be

[13] Art.29 WP Opinion 15/2011 on the definition of consent.

[14] Art.29 WP Opinion 8/2014 on the recent developments on the Internet of Things.

[15] EP report on "Big Data and Smart Devices", available online at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf.

discovered. This principle prevents arbitrary reuse[16], and calls for a "compatibility assessment of the new purpose"[17]. The 29 WP states that "*By providing that any further processing is authorised 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. 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. 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*"[17].

c. Data Minimization (Art. 5 (1) (c). 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. Organizations need to be clear about which data is deemed to be *necessary* and *relevant* for the purposes of the processing, or excessive.

e. Accurate and up-to-date processing (Art. 5 (1) (d). 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, leading to incorrect decisions (discriminatory, erroneous and unjustified, regarding their behaviour, health, creditworthiness, recruitment, insurance risk, etc.[18]). 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 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. Further, inaccuracy of data endangers the data "*quality principle*" and triggers abstract strict liability for damage [27].

f. Storage Limitation (Art. 5 (1) (e). This principle is becoming part of the *"*lifecycle governance strategy" retention policies of companies[19], such IBM, 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.

[16] 29 WP Opinion 03/2013 on Purpose Limitation, p.21.

[17] Big Data, Artificial Intelligence, Machine Learning and Data Protection, UK, ICO, 2017.

[18] Big Data, Artificial Intelligence, Machine Learning and Data Protection, UK, ICO, 2017.

[19] See http://public.dhe.ibm.com/common/ssi/ecm/wv/en/wvw12356usen/WVW12356USEN.PDF

g. Accountability (Art. 5(2). This principle requires organizations to demonstrate compliance with all the principles in the regulation, requires maintenance of records of processing activities, and to appoint a data protection officer (DPO). However, an organization's records may change as new correlations in the data are discovered which prompt different uses.

h. Privacy by design (Art. 25) is an approach in which IT system designers should code preemptive technological measures aimed to address data protection and privacy concerns applied to the very same technology that might create risks [24]. However, there is a lack of a privacy mindset in IT system designers[20], as reported by ENISA[21] "(…) *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*."

3. Conclusions

The preceding analysis brings out that smart tourism is becoming a big contributor and benefactor of ubiquitous, always-on data capture about customers towards enhanced tourism experiences, and competitive markets. The apprehension here is to understand if the affordances of the technology, the personalized services, and enhanced experiences can cope with data protection obligations without a micro-targeting and profiling. Smart tourism raises big issues with respect to information governance [18] and 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 the smart tourists who seek enriched tourism experiences [19]. 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 [12]. 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 [13]. Finally, besides addressing related information security issues according to the NIS Directive[22], future research regarding mobile devices and tracking will be needed, following the adoption of the new *ePrivacy* Regulation[23].

[20] For illustration purposes, we quote [17]"*Our findings indicate that software designers frame privacy mainly as a matter of information security (...) secrecy and internal permission systems in the organization; other principles, such as notice, consent, and rectification, were hardly found as part of the designers' perception of privacy. (...) designers perceive privacy as a theoretical-abstract concept, rather than an applicable principle in designing information systems. Moreover, they demonstrate an ambivalent attitude towards the issue whether they are responsible for addressing privacy concerns. (...) The organisational culture of commercial companies (...) ignored or discouraged consideration of PbD*".

[21] ENISA 2014 Report on "Privacy and Data Protection by Design – from policy to engineering", p.50.

[22] 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.

[23] Prop. 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).

References

[1] Bauzá Martorell, FJ. (2018), Tourism, Technology and Citizens' Legal Protection: Tourism Data, Athens Journal of Tourism, Vol. 5, Issue 1.

[2] Masseno MD (2016) 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.

[3] Manyika J. et al. (2011), Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute.

[4] Masseno M.D. (2016), 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, Fasc. 4.

[5] Gretzel, U, Reino S, et al. (2015), Smart Tourism Challenges. Journal of Tourism. Vol. 16, Issue 1

[6] Höjer, M. & Wangel, J. (2015). Smart Sustainable Cities: Definition and Challenges. In L.M. Hilty& B. Aebischer (Eds.), ICT Innovations for Sustainability, Advances in Intelligent Systems and Computing, pp. 333-349. NY, Springer.

[7] Lopez de Avila, A. (2015). Smart Destinations: XXI Century Tourism. ENTER2015 Conf. on ICT in Tourism, Lugano, Switzerland, February 4-6, 2015.

[8] Buhalis, D. &Amaranggana, A. (2014).Smart Tourism Destinations. In Xiang, Z. &Tussyadiah, I. (Eds.), ICT in Tourism 2014, pp. 553-564. Heidelberg, Germany: Springer.

[9] Buhalis, D., &Amaranggana, A. (2015). STD: Enhancing Tourism Experience Through Personalisation of Services. In Tussyadiah, I. &Inversini, A., (Eds.), ICT in Tourism 2015. Springer.

[10] Neuhofer, B., Buhalis, D., &Ladkin, A. (2015). Smart technologies for personalized experiences: a case study in the hospitality domain. Electronic Markets.

[11] Anuar, F. I. &Gretzel, U. (2011). Privacy Concerns in the Context of Location Based Services for Tourism. ENTER 2011 Conference, Innsbruck, Austria, January 26-28

[12] Schwartz, P M.; Solove, D. (2011), The PII Problem: Privacy and a New Concept of Personally Identifiable Information, NY Univ. Law Review, Vol. 86.

[13] Edwards L. (2016) Privacy, security and data protection in smart cities: a critical EU law perspective. European Data Protection Law Review, Vol. 2

[14] Habegger B, Hasan O. et al. (2014)Personalization vs. Privacy in Big Data Analysis. International Journal of Big Data, Issue 1

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

[16] Cas, J. (2009) "Ubiquitous Computing, Privacy and Data Protection" in S Gutwirth et al (2009) Computers, Privacy and Data Protection: An Element of Choice .Springer

[17] Solove, D J. (2017), 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44.

[18] Hasson T, Hadar I, et al. (2014) Are Designers Ready for Privacy by Design? Examining Perceptions of Privacy Among Information Systems Designers?", 2014 TPRC Conference Paper

[19] Tallon, P.P. (2013). Corporate governance of big data: perspectives on value, risk, and cost. Computer, 46(6)

[20] Gretzel, U., Sigala, et al. (2015) Smart tourism: foundations and developments, Electron Markets, v. 25, Issue 3

[21] Luzak, J.A. (2016), Vulnerable Travellers in the Digital Age, Journal of European Consumer and Market Law, Issue 3

[22] Davenport, Th. H. (2013), At the Big Data Crossroads: turning towards a smarter travel experience. Amadeus IT Group

[23] Leonard, P. (2014), Doing big data business: evolving business models and privacy regulation, International Data Privacy Law, Issue 1

[24] Zuiderveen Borgesius, F.J. (2016), Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation, CLSR, Vol. 32-2

[25] Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise, Computer Law & Security Review, Vol. 34-1

[26] Mantelero, A. (2015), Data protection, e-ticketing, and intelligent systems for public transport, International Data Privacy Law, Issue 4

[27] Hoeren, T. (2018) Big Data and Data Quality, in Big Data in Context - Legal, Social and Technological Insights. Hoeren, T., Kolany-Raiser, B. (Eds.), Springer.