REVISTA *ARGUMENTUM*

PERSONALIZATION AND PROFILING OF TOURISTS IN SMART TOURISM DESTINATIONS – A DATA PROTECTION PERSPECTIVE[1]-[2]

Manuel David Masseno
LabUbiNET, Instituto Politécnico de Beja (Portugal).
Cristiana Santos
JusGov, Universidade do Minho (Portugal).

Autores convidados.

ABSTRACT

This paper aims to put forward a reflection about personalization and profiling within framework of Smart Tourism Destinations (STD) and analyzing their risks to privacy and data protection given the applicability of the new General Data Protection Regulation of the EU (GDPR), as well as those coming from the ePrivacy Directive regarding mobile devices. Our main result provides a roadmap for compliance of STD design and management with the core principles embodied in the GDPR, offering guidelines both for Public and Private Sectors and for other stakeholders, namely for travellers as citizens.
KEYWORDS: *Personalization. Profiling. Privacy and Data Protection. GDPR. Regulation. Smart Tourism Destinations. Mobile Devices.*

1. INTRODUCTION

As is well known, *Smart Tourism Destinations* (hereinafter STD) are an offspring of the technological foundations of *Smart Cities*, being one of the most relevant type of *Smart Territories*. Therefore, they benefit from the interplay between other technological environments based on the *Internet of Things* (IoT) and the *Cloud*, as enabled by *Big Data Analytics*.type

Currently, companies from the travel, tourism and hospitality industry have started adopting robots, Artificial Intelligence (AI) and service automation technologies (RAISA) in

[1]This article is a major development of the paper "Assuring Compliance of European Smart Tourist Destinations with the Principles of the General Data Protection Regulation, a roadmap", accepted, following a Call for Papers, and presented at the *2nd UNWTO World Conference on Smart Destinations*, convened by the United Nation World Tourism Organization and the Government of the Kingdom of Spain, at Oviedo, the 26th June 2018.

[2]This paper was drafted within the framework of the Research Project: "*Big Data*, *Cloud Computing* y otros retosjurídicos 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 IllesBalears*, Spain.

their operations[3]. Pledging examples range from self-check-in kiosks, delivery robots, chatbots, increasingly used by tourism companies and change the ways they create and deliver services. AI and ML - Machine Learning algorithms are now an evolutionary part of personalized smart tourism: from a click-type-tap style searching, to a smart chatbot that provide hotel recommendations based on the tourists reviews and preferences[4]. Notably, *"through predictive analytics, the most favored destinations, lodging and dining preferences, ancillary services needs, and tourism experiences can be identified for each passenger. Online analytical services such as price prediction and desirability rankings can increase the likelihood of purchase."*[5]

These technology-enhanced and personalized experiences are potentiated through intensive profiling, which involve processes of information management that entail legal risks, demanding a careful analysis of the data protection framework. However, in Europe, compliance with the General Data Protection Regulation (Regulation (EU) 2016/679, hereinafter GDPR), which came into effect on 25 May 2018, forbids decision-making based on profiling which produces legal effects concerning tourists or similarly significantly affects them, such as price discrimination or denial of services.

Here, we will focus on what is profiling within STD and the risks therefrom to Data Protection and privacy. The connections between STD and Privacy & Data Protection did not receive significant attention within legal research[6], even if it was perceived and identified as an overlooked issue by tourism science[7].

---

[3] "*Robot concierges greet guests at hotel receptions, serve food as waiters in restaurants, deliver room service orders, provide information at airports, and cook food in automated kitchens. Self-service kiosks are used by hotels for check-in/out, or by travel agencies and tourist information centres for provision of information about the destination. In restaurants, customers can order food via kiosks, or tablets installed on the tables, or choose different kinds of sushi from coloured bowls moving on a conveyor belt. They can also have their pizza delivered to their home by an autonomous car or a drone. Travellers can search for travel information and book a trip via a chatbot can enter their hotel room with a mobile application on their smart phones. The speedy flow of passengers through airports is facilitated by self-check-in machines, self-service baggage drop-off, and automated passport control with face recognition"*, in: Ivanov, S. (2019). Ultimate transformation: How will automation technologies disrupt the travel, tourism and hospitality industries? Zeitschrift für Tourismuswissenschaft 11(1), (forthcoming).

[4] "*Interestingly, those using our bots treat them in a very 'human' way – ask for the bot's name, send an emoji or sticker of appreciation*." The Guardian, "Automated holidays: how AI is affecting the travel industry", 2017, accessed 05/05/2019 <https://www.theguardian.com/sustainable-business/2017/feb/17/holidays-travel-automated-lastminute-expedia-skyscanner>.

[5] DAVENPORT, Th.H. / Amadeus IT Group, At the Big Data Crossroads: turning towards a smarter travel experience, 2013 experience", accessed 05/05/2019 <http://www.amadeus.com/web/binaries/1333097571432/blobheader=application/pdf&blobheadername1=Content-Disposition&blobheadervalue1=inline%3B+filename%3DAmadeus_Big_Data.pdf>.

[6] For the legal theoretical framework of this paper, see our articles, such as MASSENO, Manuel David; SANTOS, Cristiana. "Between Footprints: Balancing Environmental Sustainability and Privacy in Smart Tourism Destinations", *Unitedworld Law Journal*, Vol. 1-II, 2017, p. 96-118, accessed 05/05/2019 <https://www.unitedworldschoollawjournal.com/wp-content/uploads/2018/05/Between-Footprints-Balancing-

The paper is organized as follows. In section 2 we explain why personalization and profiling are so important in STD. Section 3 outlines some of the most important risks raised by profiling in STD regarding privacy and data protection. Section 4 describes the obligations of the organizations processing personal data, according to the GDPR[8], which constitute the current basis of the EU-wide legal obligations regarding privacy and data protection. Section 5 refers to the compliance tools which confirm to the above-mentioned legal obligations. Section 6 deals with mobility, while Section 7 concludes the paper.

2. PERSONALIZATION IN SMART TOURISM DESTINATIONS

Tourism service providers are adapting their serviceable approach to meet personalization expectations. The implementation of smart ICT empowers tourism experience through the offer of enhanced products and services that are customized, personalized (personalized infotainment services) to meet each of the visitor's unique needs and even implied desires at an unconscious level of travelers. Notably, such tailoring is pursued since understanding travelers' needs, wishes and desires becomes increasingly critical for the attractiveness of destinations.

A data-driven customization and personalization is attained through identified venues: by collecting user-generated content (UGC), loyalty program status, travel history, past search behaviors patterns, purchase history. This crowdsourced data is harvested from technological artifacts, and reused to provide meaningful offers fitting perfectly the clients' needs, with the ultimate desideratum of achieving more satisfaction at the experience environment.

Environmental-Sustainability-and-Privacy-in-Smart-Tourism-Destinations-by-Manuel-David-Masseno-and-Cristiana-Santos-1.pdf>; and MASSENO, Manuel David; SANTOS, Cristiana. "Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations", *MediaLaws - Rivista di Diritto dei Media*, 2018, n. 2, p. 251-266, accessed 05/05/2019 <http://www.medialaws.eu/rivista/assuring-privacy-and-data-protection-within-the-framework-of-smart-tourism-destinations/>.

[7]Namely, ANUAR, Faiz I.; GRETZEL, Ulrike. "Privacy Concerns in the Context of Location-Based Services for Tourism", in *ENTER 2011 Conference. Accessibility of ICTs and Accessible Travel Information*, Innsbruck, 2001, accessed 05/05/2019 <http://agrilifecdn.tamu.edu/ertr/files/2013/02/13.pdf>; BUHALIS, Dimitrios; AMARANGGANA, Aditya. "Smart Tourism Destinations", *Information and Communication Technologies in Tourism 2014 - Proceedings of the International Conference in Dublin, Ireland*, Heidelberg: Springer, 2014, pp. 553-564, accessed 05/05/2019 <http://www.cyberstrat.net/ENTER14SmartTourismDestinations-libre.pdf>; or GRETZEL, Ulrike; SIGALA, Marianna *et al*. "Smart tourism: foundations and developments", *Electronic Markets*, Vol. 25, n. 3, 2015, pp. 179–188, accessed 05/05/2019 <https://link.springer.com/article/10.1007/s12525-015-0196-8>.

[8]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), accessed 05/05/2019 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>

Digital footprints of each customer on the travel platform allows the system to understand needs, budget and preferences of each customer, and suggest deals that are plausible and welcome. As a matter of fact, delivering the right recommendations at the right time will help reinforce customers' loyalty, keeping them coming back again and again[9]. Still, there are many possible ways to increase personalization which may be valued by traveler tourists.

Examples abound[10]: personalization based on customer behaviors (or their absence) "*We are sorry we missed you this week on the Dallas-Chicago flight after twelve straight weeks of enjoying your company!*"; personalization based on social media relationships, "*Several of your Facebook friends have recently enjoyed visits to Bermuda, so we're offering you 20% off to try it yourself*"; personalization with regard to ancillary sales, "*We know you've enjoyed our great restaurant in the past, so when you visit next week, here's a coupon for a free appetizer at it*"; personalization involving the entire journey, not just a segment of it, "*We hope you enjoy your flight to Phoenix next week. Can we interest you in a rate of $199 at the Scottsdale Princess? We'll include the limo transfer*"; personalization based on location, "*We see you have just arrived in Frankfurt Flughafen, and your final destination is Heidelberg. Did you know there is a Deutsche Bahn train that can get you there in 45 minutes*?"); personalization based on schedule disruptions, "*We are sorry to observe that you are likely to miss your flight departure. Would you like a seat in first class on the next one at 3:15PM?*").

Therefore, these STD personalized experiences are achieved through intensive profiling, context-awareness and real-time monitoring processes of *tourism-related data.* One of the main aspects needed to profile tourists is the motivations[11], behind their decision to visit a destination. Although slightly adapted to each destination because of their intrinsic characteristics, destinations attract distinct profiles of tourists, as the recreational nature-related or "sun and sand" motivations, and on the other hand, urban, cultural and gastronomic motivations. This tourism-related data, inherently cross-border, holds strategic commercial value. It comprises, for example, data:

[9] https://djangostars.com/blog/benefits-of-the-use-of-machine-learning-and-ai-in-the-travel-industry/

[10] The listed examples were extracted from the Amadeus IT Group Report "At the Big Data Crossroads: turning towards a smarter travel experience", accessed 05/05/2019 <http://www.amadeus.com/web/binaries/1333097571432/blobheader=application/pdf&blobheadername1=Content-Disposition&blobheadervalue1=inline%3B+filename%3DAmadeus_Big_Data.pdf>.

[11] Femenia-Serra, F., García-Hernández, M., del Valle Tuero, E., & Perles Ribes, J. (2018). Profiling tourists and their ICTs perception and use across Spanish destinations. In XII International Conference of Tourism and Information & Communication Technologies (Turitec) (pp. 27–46). Málaga.

i. provided directly by tourists, such as transactional data between tourists and transportation/hospitality undertakings derived from queries/searches, purchases, and other exchanges;

ii.observed about the individuals, such as location data via an application; collected via UGC profiles, established preferences, needs, etc.;

iii.derived or inferred from other data, such as a profile of a tourist that has been created through UGC, e.g. a credit score profile.

These data allow the detection and prediction of future behaviors and trends, rendering enormous interest for economic operators, and allow destinations to better plan for future tourists in terms of mobility, popular attractions, and other potential issues of tourism management. Then, STD can extract valuable insights from tourism data that could elevate them to a new dimension of customer experience and improve the way they interact with customers, hence gaining competitive advantages.

2.1. PROFILING WITHIN SMART TOURISM DESTINATIONS

Profiling is an important feature in any tourism destinations. In fact, STD data-processing scenarios collect user's input and feedback on personal preferences, interests, behavior, location, which are used to build fine-grained premium services and recommender systems in the form of trail packages. The richer the user profile, the higher the temptation for the operators to target a user with unsolicited advertising or to engineer a pricing structure capable to extract as much surplus from the user as possible[12].

But the very process of profiling is often invisible to an average tourist. It works by creating derived or inferred data about them and 'new' personal data that has not been provided directly by the tourists themselves. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes[13]. Hereby we posit the question if all profiling processes are legal.

The GDPR defines "profiling" in Article 4 as: "[…] *any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's*

[12]ENISA 2015 Report, Privacy and Data Protection by Design – from policy to engineering, accessed 05/05/2019 <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport>.

[13] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, accessed 05/05/2019, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

We follow the reasoning of profiling of the 29 Working Party to analyse the potential consequences of profiling within STD. Accordingly to the definition of the 29 Working Party, profiling has three elements:

i. it has to be an automated form of processing;

ii. it has to be carried out *on personal data*[14]; and

iii. the objective of the profiling must be *to evaluate personal aspects* about a natural person. This involves some form of assessment or judgment about a person (or group of persons) to place them into a certain category or group, in particular, or group, in particular to analyze and/or make predictions about, for example, their ability to perform a task; interests; or likely behaviour.

There are potentially three ways in which profiling may be used:

i. general profiling;

ii. decision-making based on profiling; and

iii. *solely* automated decision-making, including profiling, which produces legal effects or similarly significantly affects the data subject, Article 22(1)).

Nevertheless, data controllers can carry out general profiling and automated decision-making based on profiling, as long as they can meet all the principles and have a lawful basis for the processing as we refer to in section 4.1 (through valid consent, contract, legal obligation, etc). On the other hand, the GDPR prohibits point (iii) in specific circumstances, when a decision based solely on automated processing, including profiling, has a legal effect on or similarly significantly affects someone (as we explain in the next sub-section 2.2).

2.2. PROFILING DECISION BASED ON AUTOMATED PROCESSING WHICH PRODUCES LEGAL EFFECTS CONCERNING HIM OR HER OR SIMILARLY SIGNIFICANTLY AFFECTS HIM OR HER

This type of profiling decision making is strictly forbidden by the GDPR. In this sub-section, we will decompose this profiling decision in its three parts (according to the reasoning of Art. 29 Working Group[15]):

i. based solely on automated processing;

[14] ART 29 WP Opinion 4/2007, on the concept of personal data, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

[15] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, accessed 05/05/2019 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

ii. produces legal effects; or
iii. produces similarly significant effects

i. decision based solely on automated processing. This means that there is no human involvement in the decision process (e.g. an automated recommendation, or online advertising). To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful (rather than just a token gesture). It should be carried out by someone who has the authority and competence to change the decision, with actual influence on the result.

ii. decision producing legal effects. It requires that the decision affects someone's legal rights or obligations, such as the freedom to associate with others, vote in an election, or take legal action, or affects a person's legal status or their rights under a contract. Examples of this type of legal effect include automated decisions about an individual that result in a cancellation of a contract; an entitlement to or denial of a particular social benefit granted by law (such as child or housing benefit); refused admission to a country or denial of citizenship; or

iii. decision producing similarly significant effects. This means that even if profiling does not have an effect on citizen's legal rights, it could still produce an effect that is similarly significant in its impact. Accordingly, the effects of the processing should be significant to affect the circumstances, behavior or the choices of a tourist and/or lead to their exclusion or discrimination.

Besides, Recital 71 of the GDPR provides the following typical examples, that can easily be put into relation with tourism, and in special with STD: 'automatic refusal of an online credit application' or 'e-recruiting practices without any human intervention'. The following decisions could fall into this category: affecting someone's financial circumstances, such as their eligibility to credit, or differential pricing, based on personal data; affecting someone's access to health services; denying someone an employment opportunity or put them at a serious disadvantage; and affecting someone's access to education, for example university admissions.

Even in these cases of profiling decisions, there are defined exceptions which allow such processing to take place (when there is consent, contract or national provision). So, Recital 71 of the GDPR complements this last form of profiling; it states that such processing should be "*subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision*." These required "safeguarding measures" include the right to be informed (specifically meaningful information about the logic

involved, as well as the consequences for the tourist), and safeguards, such as the right to obtain human intervention and the right to challenge the decision (addressed in Article 22(3)).

3. PROFILING-BASED RISKS WITHIN SMART TOURISM DESTINATIONS FOR PRIVACY AND DATA PROTECTION

In this section we explain some potential risks that profiling within STD technologies entail for Privacy and Data Protection. As is increasingly valued, the use and combination of advanced techniques of *Big Data Analytics*, which include ML, data mining techniques (DM), etc., enhance the common risks to Privacy and Data Protection. 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, reviews at *Booking* or at *TripAdvisor*, blogs entries, etc.) and analysis revealed users' social interactions and activities, as is the case with smart tourist travel cards.

3.1. RISKS RELATED TO COVERT PROFILING OF TOURISTS: UNFAIR, NON-TRANSPARENT PROCESSING, AND DISCRIMINATION OF TOURISTS

For a start, the GDPR excludes automated individual decision-making that *significantly* affect individuals, Art. 22 (1). Notably, "[…] *analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behavior patterns.*"[16] Indeed, developments on consumer-tourist automated profiles, facilitated by big data analytics, can *significantly affect* data subjects[17]. Covert profiling can, in certain cases, lead to unintended consequences:

3.2. UNFAIR PROCESSING BASED IN INACCURATE DATA

If the data used in an automated decision-making or profiling process is inaccurate and/or incomplete, any resultant decision or profile can lead to false negatives, and lock a tourist into a specific category, depriving individuals from benefits that they would be entitled to, or restricting them to the company´s suggested preferences. Decisions may be made on the basis of outdated data, not trustworthy, or the incorrect interpretation of external data. Inaccuracies

[16]Art. 29 WP Opinion 8/2014, Recent Developments on the Internet of Things, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

[17]EDPS Opinion 3/2015, Europe's big opportunity, EDPS Recommendations on the EU's options for data protection reform, accessed 05/05/2019 <https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf>.

may lead to inappropriate predictions or statements about, for example, someone's health, credit or insurance risk. Even if raw data is recorded accurately, the dataset may not be fully representative or the analytics may contain hidden bias. Even exercising the "*right to be forgotten*", where data subjects have the right for their data to be erased in several situations (e.g., when the data is no longer necessary for the purpose for which it was collected, or based on inaccurate data (as set by the accuracy principle depicted in Art. 5 (1) (d)), it may in reality be difficult for a business to find and erase someone's data if it is stored across several different systems and jurisdictions.

3.3. *"*FILTER BUBBLES*"*

"Filter bubbles" effect, according to which data subjects will only be exposed to content which confirms their own preferences and patterns, without a door open to serendipity and casual discovery or spontaneity.

3.4. ISOLATION AND/OR DISCRIMINATION

In a STD, ML decisions and profiling can lead to promote direct or indirect discrimination decisions through the denial of services/goods or offering of less attractive deals than others. Examples of the former consist of: denial of insurances, exclusion from the sale of touristic services or high-end products, shops or entertainment complexes to certain profiled tourists, and even targeting with excessively risky or costly products.

Also, ML-based systems used in STD can render automated decisions that could reflect upon health, creditworthiness, taxation, recruitment, insurance risk, etc. An example of a real-life setting is provided by the ART. 29 WG that could easily be transposed to a data broker compiling consumer tourism profiles: *"A data broker sells consumer profiles to financial companies without consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Tough Start: Young Single Parents,") or "score" them, focusing on consumers' financial vulnerability. The financial companies offer these consumers payday loans and other "non-traditional" financial services (high-cost loans and other financially risky products)"*

Even more, profiling within STD can lead to exclude the access to utilities for those unwilling to share personal data. Also, travelers might be discriminated against because 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. As such, profiling can perpetuate stereotypes and social segregation.

Have in mind that Big Data algorithms (also used in STD scenarios) learn and change in a (semi) autonomous way, making them hard to document; further, organizations often claim secrecy over "how" data is processed on grounds of commercial confidentiality and copyright protecting the software and the trade-secret shield. Hence, profiling and correlation results are invisible and opaque, and its results often impenetrable to laymen, which is left without meaningful information about the employed "algorithmic logic".

3.5. IDENTIFICATION AND RE-IDENTIFICATION OF INDIVIDUALS FROM ALLEGEDLY ANONYMIZED OR PSEUDONYMIZED DATA

These concerns stem from 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 re-identification; this scenario could escalate if massive information resources via the web are available[18].

Thereby, personal information set through reidentification intrinsically conforms with 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[19]. As data collected by the ubiquitous computing sensors is, in principle, personal data 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.

3.6. REPURPOSING OF DATA AND FURTHER PROCESSING

Profiling can involve the usage of personal data that was initially collected for something other purpose[20]. As an illustrative example, "*Some mobile applications provide location services allowing the user to find nearby restaurants offering discounts. However, the data*

[18]ART 29 WP – Article 29 Working Party of the European Union: Opinion 7/2003, on the re-use of public sector information, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf>; Opinion 3/2013, on purpose limitation, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>; and, Opinion 6/2013, on open data and public-sector information (PSI) reuse, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf>.

[19]ART 29 WPOpinion 05/2014, on anonymization techniques, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

[20] ART 29 WP Opinion 3/2013, on purpose limitation, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

collected is also used to build a profile on the data subject for marketing purposes - to identify their food preferences, or lifestyle in general. The data subject expects their data will be used to find restaurants, but not to receive adverts for pizza delivery just because the app has identified that they arrive home late. This further use of the location data may not be compatible with the purposes for which it was collected in the first place, and may thus require the consent of the individual concerned"[21].

3.7. PREDISPOSITION TO COLLECT, ANALYZE AND STORE ALL DATA

The tourism industry is inherently based on data-exchange to create very comprehensive refined and intimate profiles of individuals, and thus, datasets need to be as exhaustive and varied as possible to faithfully reflect tourist activity within a territory.

In substance, smart technology undertakes the extensive collection, aggregation, algorithmic analysis and retention of all the available data for profiling (e.g. profiles of customer purchasing behaviour), hampering the data minimization and storage principles (Art. 5 (1)(c)(e)). In addition, irrelevant data is also being collected and archived, undermining the storage limitation principle (Art. 5 (1) (e)).

3.8. FAILED CONSENT

Within this sort of Intelligent Territories, is awkward to give or withhold our prior consent to data collection, as it seems to be absent by design. These ubiquitous sensors are so embedded in the destination that there is little awareness of them, or none at all; thus, they literally "disappear" from the users' sight. Users will not even be conscious of their presence and hence the notion of consent to the collection of data is problematic.

We may, at least to some extent, concede that obtaining such consent, in STD contexts, would be achievedin a mechanical or perfunctory manner, or as a "routinization". We also perceive with regard to CCTV, ANPR and MAC whilst tracking and sensing that notice in the form of information signs in the area being surveilled, or on related websites, wouldnot conform to the consent requirements. Thus, the main issue of the *IoT* embedded in STD is that its sensorization devices are explicitly designed to be unobtrusive and seamless, invisible in

[21] Transcribed example from the ART 29 WP Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, accessed 05/05/2019, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

use and imperceptibleto users and thereupon, users do not have the opportunity to give their unambiguous, informed, specific, explicit, and granular consent[22].

Therefore, the data controller might have difficulty in demonstrating that consent was given, and the data subject is not able to withdraw that consent. Still, consent is not yet part of a function specification of *IoT* devices, and thus, they do not have the means to *"*provide fine-tuned consent in line with the preferences expressed by individuals,*"* because smart roads, trams, tourist office devices are usually small, screenlessand lack an input mechanism (a keyboard or a touch screen)[23].

4. THE OBLIGATIONS OF ORGANIZATIONS WHILE PROCESSING PERSONAL DATA WITHIN A STD

While realizing the benefits of profiling and being a competitive STD, addressing data protection concerns supports best practices in information governance. Accordingly, it is in the interests of Destinations to pay careful attention to these issues. Therefore, Data Protection compliance should hence be viewed as an enabler of the success of an STD and not as a regulatory or procedural burden.

By now is widely known that (Art. 83), infringement or non-compliance with the GDPR may lead to fines up to €20 million or 4% of the worldwide annual revenue of the prior financial year, whichever is higher. This, along with a system of full compensation of all damages and strict liability, meaning that a fault of the controller or the processor is not required (Art. 82).

As stated in the tourism literature, tourism, by definition, is a service-intensive industry with a "*business network*", since it relies on a number of stakeholders for its ability to deliver products and services. In these networks, each of the actors involved in the transportation, accommodation, gastronomy, attractions and ancillary services, potentially process personal data.

For a STD, the public or private organizations that decide the "whys" and "hows" by which the personal data is tobe processed are called "data controllers". They may use other parties that process personal data on their behalf, called "data processors". Both data

[22]ART 29WP Opinion 15/2011, on the definition of consent, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>; updated by its Guidelines on Consent under Regulation 2016/679, accessed 05/05/2019 <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030>.

[23]ART 29 WP Opinion 8/2014, on the Recent Developments on the Internet of Things, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

controllers and data processors must abide by the GDPR obligations. However, Big Data Analytics can make it difficult to distinguish between controllers and processors; further, within the modern data value chain, organizations outsourcing analytics and AI to specialized companies need to consider carefully who has control over the processing of any personal data (Art. 4 (7) (8)). Therefore, if an organization chooses to store its customer data in the cloud, then the cloud provider is likely to be a data processor, as it is acting on the original organization's behalf, and it is not determining the purpose of the processing. Hence, if an organization aims to conduct its analytics outsourcing in a data controller-data processor relationship, it is important that the contract includes clear instructions about how the data can be used and the specific purposes for which it is being processed. Nevertheless, it does not follow from the existence of a contract of this type that the sub-contracted company performing data analysis is a data processor; if this company uses its discretion and expertise to decide what data to collect and how to apply its analytic techniques, then it is very likely to be a data controller as well; in facta co-controllership[24] (Art. 24).

Under the accountability principle (Art. 24), data controllers shall be responsible for, and be able to demonstrate compliance with, all the obligations and principles contained in the regulation. Some of its most important obligations are explained below.

4.1. FAIR, LAWFUL AND TRANSPARENT PROCESSING OBLIGATIONS

STD organizations must process personal data "fairly, lawfully and in a transparent manner in relation to the data subject" (art. 5 (1) (a) of the GDPR), i.e., when the data is collected, it must be clear as to why that data is being collected and how the data will be used. Whether the data is volunteered, observed, inferred, individuals are fully entitled to know what it is, from where and from whom the controllers obtained it, and how automated decisions were taken in relation to it. Also, the controller must provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data (under Art. 12(1), and within the timescale set out in Art. 14(3)).

In order to ensure a *fair and transparent*[25] processing, automated decisions should take account of all the circumstances surrounding the data and not be based on merely de-contextualized information or on data processed results. The controller should furthermore

[24]ICO (Information Commissioner's Office, of the United Kingdom)Guideon Big data, artificial intelligence, machine learning and data protection, 2017, accessed 05/05/2019 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

[25] ART 29 WP Guidelines on transparency under Regulation 2016/679, accessed 05/05/2019 <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850>.

build discrimination detection into their ML systems, to prevent inaccuracies and errors being assigned to labeled profiles, as referred in Recital 71 of GDPR.

Regarding a *lawful processing,* automated decision-making including profiling, which produces legal effects concerning a tourist or similarly significantly affects him is *only* permitted when:

i. is necessary for entering into, or performance of, a contract between the traveler and a data controller. It may be difficult to show that big data analytics in STD are strictly necessary for the performance of a contract, since the profiling goes beyond what is required to sell a product or deliver a service;

ii. is based on the tourist explicit consent[26]. Data subjects should have enough relevant information on the envisaged use and risks of the processing to ensure that any consent they provide represents an informed choice;

iii. there is EU or national legislation permitting it, e.g. for monitoring and preventing fraud and tax-evasion, or to ensure the security and reliability of a service provided by the controller (recital 71).

The following lawful bases for processing are relevant for all other automated individual decision-making and profiling (that do not affect travelers) (Art. 6):

i. consent;
ii. necessary for the performance of a contract;
iii. necessary for compliance with a legal obligation, e.g. in connection with fraud prevention or money laundering;
iv. necessary to protect vital interests, e.g. e.g. when the profiling is necessary to develop models that predict the spread of life-threatening diseases or in situations of humanitarian emergencies;
v. necessary for the performance of a task carried out in the public interest or exercise of official authority;
vi. necessary for the legitimate interests[27] pursued by the controller or by a third party.

[26] Article 29 Data Protection Working Party. Guidelines on Consent under Regulation 2016/679, accessed 05/05/2019 <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849>.

[27] Art. 29 WP Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, accessed 05/05/2019 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>.

Most commercial systems rely on the latter basis even if they consist of "the vaguest ground for processing". This provides a considerable scope for industry to process data by claiming any purportedly necessary "legitimate interest". In fact, the processing must be "necessary" for legitimate interests and not just *potentially* interesting for the operator. Besides, the ART 29 WP acknowledges that it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering. It follows that the processing is unnecessary if there is any other means of meeting that legitimate interest which interferes less with public privacy. So, the controller must carry out a *balancing exercise* to assess whether their interests are overridden by the data subject's interests or fundamental rights and freedoms.

A close attention should also be given to the level of detail of the profile (granular profile or broadly described); the comprehensiveness of the profile (whether the profile only describes a small aspect of the data subject, or paints a more comprehensive picture); the impact of the profiling (the effects on the data subject)[28].

4.2. ALGORITHMIC ACCOUNTABILITY

Organizations should also check "algorithmic accountability", which means being able to check that the algorithms used and developed by machine learning (ML) systems are actually doing what we think they are doing (and are not producing discriminatory, erroneous or unjustified results), under the right to know the "logic of the processing" applied to data (Recital 63, and Arts. 13(2) (f), and 15(1) (h)), respectively, as the GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. This information should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.

So, organizations using ML techniques in STD are obliged to assure data quality by checking the sources of the data, the accuracy of the data, whether is sufficiently up to date, how securely it is kept, and whether there are restrictions on how it can be used (anonymized data).

[28] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, accessed 05/05/2019 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

4.3. APPOINTING A DATA PROTECTION OFFICER

The GDPR mandates the appointment of a Data Protection Officer (DPO) within the organization whose responsibilities include: monitoring data governance and privacy, providing advice, monitoring data protection impact assessments, and acting as the point of contact with any supervisory authority. This is mandatory where the processing is carried out by a public authority or body, except for the courts; their core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or processing on a large scale of special categories of data (Articles 37 to 39)[29].

4.4. PURPOSE LIMITATION

The principle of purpose limitation is to ensure that the purpose for which the data is collected is specified and lawful. This principle also prevents arbitrary re-use, which means that personal data should not be further processed in a manner that the data subject might considered unexpected, inappropriate or otherwise objectionable[30] and therefore unrelated to the delivery of the service. In other words, exposing data subjects to different/greater risks than those contemplated by the initial purposes maybe considered to amount to the further processing of data in an unexpected manner[31].

4.5. DATA MINIMIZATION AND RETENTION OBLIGATIONS

Data minimization means that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (Art. 5 (1) (c)). This obligation means that STD entities should minimize the amount of data they collect and process, and the length of time they keep the data. Even if, in practice, smart technology envisages the massive collection, aggregation and algorithmic analysis for profiling purposes, controllers should be able to explain and motivate the need to collect and hold personal data, or consider using aggregated, anonymised or (when this provides enough protection) pseudonymized data for profiling.

As for *data storage*, personal data shall not be kept (stored) longer than necessary for the purpose for which it is being processed, as prescribed by the storage limitation principle (Art.

[29]ART 29 WP Guidelines on Data Protection Officers ('DPOs'), accessed 05/05/2019 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44100>.
[30]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, accessed 05/05/2019 <https://rm.coe.int/16806ebe7a>.
[31]ART 29 WP Opinion 3/2013, on purpose limitation, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>

5 (1) (e)). This obligation is part of the lifecycle governance strategy retention policies of companies that defensibly dispose of irrelevant data rather than keeping data archived forever. Regarding retention timeframes, retention schedules allow unnecessary data to be disposed of, as it is no longer of business value or needed to meet legal obligations. Data mapping techniques may permissibly identify where and what type of data is stored within an organization. Data management segmentation can also help to segregate EU data from data coming from other data subjects.

4.6. ACCURACY AND UP TO DATE PROCESSING OBLIGATIONS REGARDING PROFILING

Controllers should consider accuracy at all stages of the profiling process, specifically when: collecting data; analysing data; building a profile for an individual; or applying a profile to decide affecting that person.

If sources of data are reliable, accurate and representative, so too must be the results drawn from big data analysis employed in a STD environment (Art. 5 (1) (d)). For example, analysis based on social media sources are not necessarily representative of the population as a whole[32].

Destinations deploying ML algorithms need to consider the distinction between correlation and causation[33], *i.e.*, when there is no *direct cause and effect* between two phenomena that show a close correlation. In these cases, there is a risk of drawing inaccurate, but also – and when applied at the individual level – potentially unfair and discriminatory conclusions[34]. The potential accuracy (or inaccuracy) of any resulting decisions might cause discriminatory, erroneous and unjustified decisions regarding the data subject´s behavior in relation to their health, creditworthiness, recruitment, insurance risk, etc. Thus, the quality of the profiles and of the personal data upon which they are built, again, seem to matter just for the success of the industry.

Controllers also need implement measures to verify and ensure that data reused and/or obtained indirectly is accurate and up to date. This reinforces the importance of providing clear information about the personal data being processed, so that the data subject can correct any inaccuracies and improve the quality of the data.

[32]ICO Guideon Big data, artificial intelligence, machine learning and data protection, 2017, accessed 05/05/2019 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>
[33]ICO Guide on Big Data, cit.
[34]EDPS Opinion 7/2015 on Meeting the challenges of big data, accessed 05/05/2019 <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf>

4.7. DATA BREACH REPORTING

EU data protection law requires controllers to promptly notify the relevant supervisory authority and the data subjects of potential data breaches in the event of causinga high risk to data subjects. The notification must include at least: the name and contact details of the DPO (or other relevant point of contact); the likely consequences of the data breach; and any measures taken by the controller to remedy or mitigate the breach. However, the controller may be exempt from this requirement if the risk of harm is remote because the affected data are protected (e.g., due to strong encryption). Most importantly, if the risks associated with the breach have been effectively resolved, then the organization may be exempt from the notification requirements[35].

4.8. PROCESSING ACTIVITIES RECORDS

EU data protection law requires organizationsinvolved in STD to keep records (written or electronic) of their data processing activities (Art.30). Examples of records to be kept include the purposes of the processing; the categories of data subjects and personal data processed; and the categories of recipients with whom the data may be shared. Upon request, these records must be disclosed to, National, Data Protection Authorities.

4.9. CODES OF CONDUCT AND CERTIFICATION MECHANISM

In order to enhance transparency and compliance with this Regulation, associations and other institutional bodies representing both controllers and processors are obliged to elaborate codes of practice specifying how the GDPR should be applied. These bodies must then submit their draft codes of conduct to the relevant supervisory authority for approval.

Besides, the GDPR introduced certification mechanisms and data protection marks, allowing data subjects to quickly assess the level of data protection employed by the products and services in question. A list of certified organizations will thus be publicly available. Codes of conduct and approved certification mechanisms will also assist controllers in identifying the risks related to their type of processing and in adhering to best practices.

[35]ART 29 WP Guidelines on Personal data breach notification under Regulation 2016/679, accessed 05/05/2019 <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827>.

5. COMPLIANCE TOOLS AT THE GDPR

Compliance tools enable STD organizations to meet their data protection obligations while protecting people's privacy rights in a STD context. These are: anonymization and pseudonymization techniques, privacy policies, data protection impact assessment (DPIA), personal data stores, algorithmic transparency, privacy seals/certification, and privacy by design (PbD) measures to mitigate identified legal risks and implications. STD managers may demonstrate commitment to compliance through internal documentation and employee training in relation the GDPR-related mandates, such as via written internal policies.

5.1. ANONYMIZATION

As a stated 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 allows no possibility to re-identify the person(s) concerned. Consequently, it is deemed to be no longer personal data. Later, anonymised data might be aggregated in order to be analysed and to gain insights about the population, as well as combined with data from any other sources. At this stage, *IoT* developers can analyse, share, sell or publish the data without any 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.

In what has to do with *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[36].

5.2. PRIVACY POLICIES

Privacy policies consist of documents which set forth 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 and as a "tool for preference-matching" for consumers, as consumers tend toplace a higher value on a product/service, after learning more about its attributes and tradeoffs. As such, Privacy Policies constitute the *locus* where

[36]ART 29 WPOpinion 05/2014, on anonymization techniques, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

consequences are produced, the "technically most feasible place to protect privacy and personal data"[37].

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, visualization is used" (Article 12(7) and Recital 60).

However, in a STD scenario, these requirements can be problematic, and it has been suggested that privacy notices are not feasible when Big Data Analytics are entailed, given that: travelers engaged in tourism are unwilling to read lengthy legalese such as privacy notices, since it would take significantly more time than they spend using the content or the app itself; 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 typeof these interactions, it is just too onerous for each data subject to assess their privacy settings across dozens of entities in order to ponder 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. On the other hand, information can be delivered in a user-friendly form, namely by: 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[38].

5.3. 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 involves description of the envisaged processing operations, an evaluation of the privacy risks and the measures contemplatedto address those risks.

Art. 35 of GDPR indicatesthat when a type of processing which uses a systematic and extensive evaluation of individuals based on automated processing and profilingis 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

[37] President's Council of Advisors on Science and Technology, Big Data and Privacy: a Technological Perspective. Executive Office of the President, USA (2014), accessed 05/05/2019 <https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf>.

[38] ART 29 WP Opinion 8/2014, on the Recent Developments on the Internet of Things,accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

protection of personal data. It is likely that general big data applications within an STD involving the processing of personal data will fall into this category[39].

5.4. PRIVACY BY DESIGN

By design solutions (PbD) is an approach in which IT system designers seek to adopt preemptive *technological* and *organizational* measures to protect personal data, when designing or creating new products and services. By design solutions are necessary at the early development stage (planning and implementation) of any new product or service that affects personal data. It aims to address privacy concerns attachedto the very same technology that might create risks (Art. 25).

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; as well as sticky policies whichrecord individual preferences, and corporate rules within the metadata that accompanies data.

Within a STD scenario, controllers and processors should test the adequacy of the above-mentioned solutions bydesign on a limited amount of data by means of simulations before they are used on a larger scale. Such a learn-from-experience approach makes it possible to assess the potential bias inherent in using different parameters in analyzing data, and provides a rational for minimising the use of information. However, there is a lack of a privacy mindset in IT system designers. As 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 realize privacy by design. While the research community is very activeand growing, and constantly improving existing and contributing further building blocks, it is only loosely interlinked with practice*."[40]

[39]ART 29 WP Guidelines on Data Protection Impact Assessment (DPIA), accessed 05/05/2019 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.
[40]ENISA Report on Privacy and Data Protection by Design – from policy to engineering,accessed 05/05/2019 <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport>.

5.5. 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, which are oftenprovidedby personal information management services[41].

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.This tool aims to address criticisms related to the lack of control over 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 do not have the time to read privacy notices.

5.6. ALGORITHMIC TRANSPARENCY

The following suggestions concerning algorithmic transparency are reflected in the research findings of the UK's Information Commissioner´s Office[42]: 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 boardscan be used to help shape and improve the transparency of the development of machine learning algorithms.

5.7. CODES OF CONDUCT, PRIVACY SEALS AND CERTIFICATION

Within each STD, a code of conduct should be adopted, being of mandatory subscription by any interested organization or business. Furthermore, certification schemes (Arts. 42, 43, Recital 100) can be used to help demonstrate 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

[41]EDPS Opinion 7/2015 on Meeting the challenges of big data, accessed 05/05/2019 <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf>

[42]ICO Guide on Big Data, cit. Guideon Big data, artificial intelligence, machine learning and data protection, 2017, accessed 05/05/2019 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

operations comply with the Regulation. These are awarded by data protection authorities or by accredited certification bodies[43].

6. MOBILE DEVICES

Another specific key-issue within STD comes out of the almost universal use of mobile devices, mostly smartphones ad tablets by travelers. In short, almost every tourist carries a terminal, at least. Hence, with the location and interaction taking place through these devices.

However, along with the GDPR, for these purposes, the ePrivacy Directive[44]-[45] must be taken into consideration, as, according to Article 1(2), "this Directive particularise and complement Directive 95/46/EC", the previous Legal Instrument regarding Data Protection. Therefore, the GDPR may not "impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective", Article 95.

6.1. GEOLOCATION

For STD, geographical information related to the actual location of travelers has an upmost relevance, mostly to adjust services to their potential demands, by following their

[43]ENISA 2017 Recommendations on European Data Protection Certification, accessed 05/05/2019 <https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullRepor>.

[44]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 ('Citizens Directive'), accessed 05/05/2019 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058>.

[45]About these legal Instruments, ART 29 WP Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf>; Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp126_en.pdf>; Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), accessed 05/05/2019<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp150_en.pdf>;Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), accessed 05/05/2019 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_en.pdf>; and Opinion 03/2016 on the evaluation and review of the ePrivacy Directive, accessed 05/05/2019<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf>.

behavior in real time. Specifically, this data is obtained and shared in order to provide shared services as maps, including references to the nearest points of interest, possibly enhanced with augmented reality, or the location of other people, namely nearby friends or children that departed for short explorations on their own. Technically, this location services lay on a combined framework of GPS, GSM base stations and Wi-Fi points of access.

As everybody, or almost, carry along their mobile devices permanently, this data permits the built of detailed profiles, including those of related persons, through *social-graphs*, leading to increased privacy risks.

Article 2 of the ePrivacy *Directive* defines "location data" as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service". However, this only applies to the processing of personaldata in connection with the provision of publicly available electronic communications (Art. 4). So, within a STD, a close cooperation of each tourism related service provider with telecom operators has to be promoted, in order to provide a clear and common interface for travellers to manage their consent options, according to their desired privacy levels, in general or for each provider. Notwithstanding, common settings related to anonymization, pseudonymization and minimization, as well as to the eventual erasure of data, should also be designed at each STD[46].

6.2. GEOREFERENCED SERVICES APPS

Currently, the most usual interface of travelers with tourism services providers are the apps, software applications designed for specific tasks, present at each smart mobile device. Adding to these, apposite apps are usually provided by STD, for the coordination of the single providers.

However, these apps convey relevant privacy risks, mostly related to the huge amount of data being processed and to the access to core services of the device, such as address books and locations, made available by Applications Programming Interfaces. Besides, apps also connect through network interfaces as Wi-Fi, Bluetooth, NFCor Ethernet. So, at STD, the

[46]ART 29 WP Opinion 5/2005 on the use of location data with a view to providing value-added services,accessed 05/05/2019<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf>; and Opinion 13/2011 on Geolocation services on smart mobile devices, accessed 05/05/2019<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf>.

stated requirements regarding "privacy by design" and "privacy by default" must be taken seriously. This, both for STD own apps and to local tourism related services providers apps, even putting in place a certification procedure for the later. In any case, a key feature would be a reduced access to geolocation data, with specific and time limited consent required, along with strict purpose limitation and data minimisation[47].

6.3. THE FUTURE EPRIVACY REGULATION

Having regard for the shortcomings of ePrivacy Directive, the European Commission presented a Proposal for a new ePrivacy Regulation[48], the 10th January 2017. According to the *Proposal*, the *New Regulation* will have a relevant effect on geolocation related rules, as Over-The-Top services are included. Besides, and with a highest impact, the tracking of the devices might take place without the consent of the person concerned, the allowed scope of the collected data and subsequent processing activities are not clear, the same for the need of consent related to metadata[49]. Yet, we should wait for the final agreement between the EU Institutions before an accurate analysis of the New Regulatory Ecosystem regarding ePrivacy.

7. SOME CONCLUSIONS

The preceding analysis emphasizes that Smart Rourism is becoming a major contributor to, and benefactor of, ubiquitous, always-on data capture about customers, aimed at enhanced tourism experiences, and increasing competitiveness, already based on AI.

---

[47] ART 29 WP Opinion 02/2013 on apps on smart devices, accessed 05/05/2019<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>.

[48] 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 and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final, of 10.01.2017, 05/05/2019 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>.

[49] ART 29 WP Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), following Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), accessed 05/05/2019 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44103>; Opinion of the European Economic and Social Committee on the '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 and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (COM(2017) 10 final — 2017/0003, accessed 05/05/2019 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017AE0655>; Opinion of the European Data Protection Supervisor on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), accessed 05/05/2019 <https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf>; and, finally, Statement 3/2019 on an ePrivacy regulation, of the new EDPB – European Data Protection Board, accessed 05/05/2019 <https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf>.

However, 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, including geolocation, and to the profiling of travelers, all in real time. Even, this is made on *Good Faith*, to deliver personalized experiences for each costumer and not with the sole objective of increasing the revenues of business or the control of the whereabouts of citizens, GDPR and ePrivacy compliance is mandatory

Therefore, our foremost concern was to provide an in depth understanding of the main sensitive Data Protection related risks, namely those related to the profiling of travelers, as well as of the available compliance tools. Of course, we could have taken another approach, for instance taking the perspective of the rights of the travelers, as data subjects, regarding STD and / or addressing the issues related to special categories of data, but that would unbalance the article and divert the readers from the central issues under analysis.